

HARD DISK UNIT

Publication number: JP2003248557 (A)

Publication date: 2003-09-05

Inventor(s): HORI YOSHIHIRO; HIOKI TOSHIAKI

Applicant(s): SANYO ELECTRIC CO

Classification:

- international: G06F12/14; G06F3/06; G06F21/24; G09C1/00; G11B19/12; G11B20/00; G11B20/10; G11B20/12; G11B5/012; G06F12/14; G06F3/06; G06F21/00; G09C1/00; G11B19/12; G11B20/00; G11B20/10; G11B20/12; G11B5/012; (IPC1-7): G06F3/06; G06F12/14; G09C1/00; G11B20/10; G11B20/12

- European: G11B19/12C; G11B20/00P; G11B20/10

Application number: JP20020049763 20020226

Priority number(s): JP20020049763 20020226

Also published as:

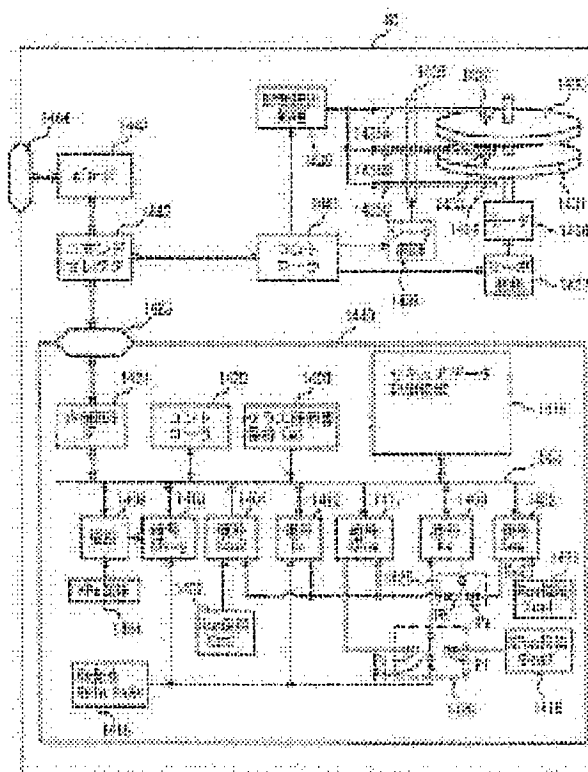
US2003161064 (A1)

CN1441590 (A)

Abstract of JP 2003248557 (A)

PROBLEM TO BE SOLVED: To provide a hard disk unit capable of fully protecting confidential data. ;

SOLUTION: A hard disk unit 40 stores encrypted contents data into hard disks 1430 and 1431 by a storage reading processing part 1439 and a license for decoding the contents data is stored into a secure data area 1415 in a storage element 1440. The storage element 1440 is composed of semiconductor elements, and hard disk units 40 and 41 are accessible independently. ; COPYRIGHT: (C) 2003,JPO



Data supplied from the esp@cenet database — Worldwide

(11)特許出願公開番号

特開2003-248557

(P2003-248557A)

(43)公開日 平成15年9月5日(2003.9.5)

(51)Int.Cl. ⁷	識別記号	F I	データベース*(参考)
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06	3 0 4 M 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 B 5 B 0 6 5
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 D 5 D 0 4 4
G 1 1 B 20/10		G 1 1 B 20/10	D 5 J 1 0 4
			H

審査請求 未請求 請求項の数5 OL (全 30 頁) 最終頁に続く

(21) 出願番号 特願2002-49763(P2002-49763)

(22)出題日 平成14年2月26日(2002.2.26)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72) 發明者 堀 吉宏

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(72) 發明者 日置 敏昭

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

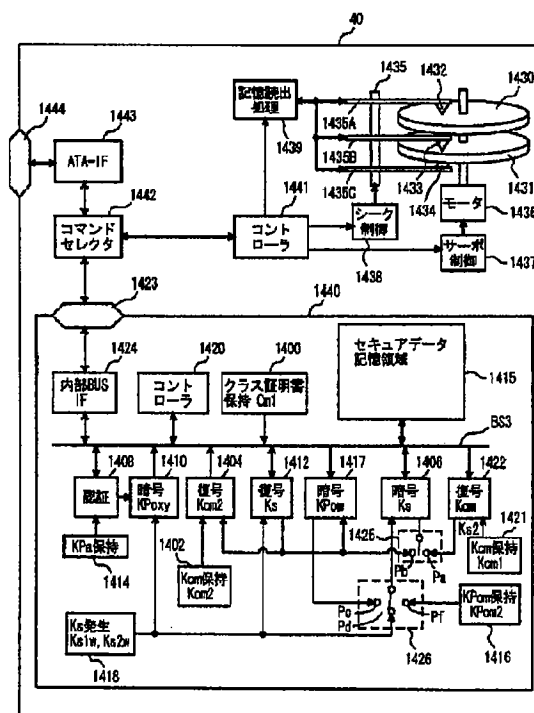
[最終頁に続く](#)

(54) 【発明の名称】 ハードディスクユニット

(57) 【要約】

【課題】 機密データを十分に保護可能なハードディスクユニットを提供する。

【解決手段】 ハードディスクユニット４０においては、暗号化コンテンツデータは、記憶読出処理部１４３９によってハードディスク１４３０、１４３１に記憶され、暗号化コンテンツデータを復号するためのライセンスは記憶素子１４４０のセキュアデータ記憶領域１４１５に記憶される。そして、記憶素子１４４０は半導体素子として構成され、ハードディスクユニット４０、４１とは独立してアクセス可能である。



【特許請求の範囲】

【請求項 1】 機密データと非機密データとの入出力を行ない、かつ、前記機密データと前記非機密データとを記憶するハードディスクユニットであって、外部とのデータの授受を行なうインタフェースと、外部の他の装置とデータをやり取りする端子と、前記端子を前記インタフェースに接続するデータバスと、

前記機密データを記憶し、不正なアクセスから前記機密データを保護する記憶素子と、前記非機密データを記憶する円盤状磁気記憶媒体と、前記非機密データを前記円盤状磁気記憶媒体に記憶および／または読出を行なう記憶読出処理部とを備え、前記記憶素子は、

前記機密データを記憶するデータ記憶部と、前記機密データを入出力する場合に、前記機密データの提供元または提供先との間で暗号路を構築し、かつ、機密データの入出力に関するデータ管理部とを含む、ハードディスクユニット。

【請求項 2】 前記記憶素子は、独立した半導体素子によって構成される、請求項 1 に記載のハードディスクユニット。

【請求項 3】 前記記憶素子は、当該ハードディスクユニットから着脱可能である、請求項 1 または請求項 2 に記載のハードディスクユニット。

【請求項 4】 前記機密データの入出力処理に関するデータの授受を前記インタフェースと前記記憶素子との間で仲介し、前記非機密データの入出力処理に関するデータの授受を前記インタフェースと前記記憶読出処理部の間で仲介する選択部をさらに備える、請求項 1 から請求項 3 のいずれか 1 項に記載のハードディスクユニット。

【請求項 5】 前記インタフェースは、前記機密データを外部との間で授受する第 1 のインタフェースと、前記非機密データを外部との間で授受するための第 2 のインタフェースとを含み、

前記端子は、前記他の装置とデータをやり取りする第 1 の端子と、前記第 1 の端子を前記第 1 のインタフェースに接続する第 1 のデータバスと、前記他の装置とデータをやり取りする前記第 1 の端子から独立した第 2 の端子と、前記第 2 の端子を前記第 2 のインタフェースに接続する第 2 のデータバスとを含む、請求項 1 から請求項 4 のいずれか 1 項に記載のハードディスクユニット。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生する

ためのライセンスを記憶するハードディスクユニットに関し、特に、マルチアクセスが可能な記憶装置においてコピーされた情報に対する著作権保護を可能とするハードディスクユニットに関するものである。

【0002】

【従来の技術】 近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】 このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】 したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】 一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】 しかし、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0007】 この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0008】 そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスを送信する。ライセンスは、暗号化コンテンツデータを復号するための復号鍵（「コンテンツ鍵」と言う。以下同じ。）と、ライセ

ンスを識別するためのライセンスID、およびライセンスの利用を制限するための制御情報等を含んでいる。配信サーバからメモリカードに対してライセンスを送信する際には、配信サーバおよびメモリカードは、それぞれがセッション鍵を生成し、配信サーバとメモリカードとの間で鍵の交換を行なうことによって、暗号通信路を構築する。

【0009】最終的に、配信サーバはメモリカードに対して構築した暗号通信路を介してライセンスを送信する。その際、メモリカードは、受信した暗号化コンテンツデータとライセンスとを内部のメモリに記憶する。

【0010】メモリカードに記憶した暗号化コンテンツデータを再生する場合は、メモリカードを携帯電話機に装着する。携帯電話機は、通常の通話機能の他にメモリカードから暗号化コンテンツデータとコンテンツ鍵を読み出して暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。ライセンス鍵の読み出しに際しては、メモリカードと専用回路との間に暗号通信路を構築し、暗号通信路を介してメモリカードから専用回路に送信される。

【0011】また、メモリカードは、他のメモリカードとの間でライセンスの移動または複製を行なう機能を備えている。この場合、配信サーバからライセンスの送信と同様に、送信元のメモリカードと送信先のメモリカードの双方の機能によって暗号通信路を構築した上で、ライセンスが送信元のメモリカードから送信先のメモリカードに対して送信される。ライセンスを移動するか複製するかは、ライセンスに含まれる制御情報に従って決定される。

【0012】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータとライセンスとを配信サーバから受信し、メモリカードに記憶したうえで、メモリカードに記憶された暗号化コンテンツデータを再生したり、他のメモリカードに移したりできる。

【0013】また、近年、放送網のデジタル化、デジタル通信路の広帯域化によって大量なデータの送信が可能となりつつある。このようなデータ送信環境の変化によって、これまで、音楽データのように比較的データ量の少ないコンテンツデータから、大容量な映像データの配信を行なうことができるインフラストラクチャーが整いつつある。

【0014】一方、メモリカードは、映像データを扱う場合には、データ記憶容量が少ない、データのアクセス速度の遅いデータに対する1ビット当りの記憶単価が高いなどの性能・価格の面から見ると、映像データを扱うには最適な記憶メディアであるとは言いがたい。

【0015】大記憶容量、高速アクセス、かつ、1ビット当りの記憶単価が安い記憶メディアとしてハードディスクユニットが存在する。

【0016】

【発明が解決しようとする課題】しかし、現行のハードディスクユニットは、ライセンスのような機密性を要する機密データを記憶する媒体としては、その機密性が低いという問題がある。

【0017】また、ハードディスクユニットは、内部にモータなどの能動部品を備えているために装置寿命が短いこと、耐衝撃性が低く、ユニット内部に備えられている磁気記録媒体であるハードディスクユニットの損傷によってハードディスクユニット上の記憶されたデータが容易にアクセス不能となることから明らかなように、ライセンスのようにバックアップを取ることが許されないデータそのものの価値のある機密データを扱うには、記憶の安全性が低いという問題もある。

【0018】そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、ハードディスクのように記憶されたデータが読出不能となった場合でも、記憶されている機密データに対するアクセスを保証し、機密データに関する記憶の安全性を確保するハードディスクユニットを提供することである。

【0019】

【課題を解決するための手段】この発明によれば、ハードディスクユニットは、機密データと非機密データとの入出力を行ない、かつ、機密データと非機密データとを記憶するハードディスクユニットであって、外部とのデータの授受を行なうインタフェースと、外部の他の装置とデータをやり取りする端子と、端子をインタフェースに接続するデータバスと、機密データを記憶し、不正なアクセスから機密データを保護する記憶素子と、非機密データを記憶する円盤状磁気記憶媒体と、非機密データを円盤状磁気記憶媒体に記憶および／または読出を行なう記憶読出処理部とを備え、記憶素子は、機密データを記憶するデータ記憶部と、機密データを入出力する場合に、機密データの提供元または提供先との間で暗号路を構築し、かつ、機密データの入出力に関するデータ管理部とを含む。

【0020】好ましくは、記憶素子は、独立した半導体素子によって構成される。好ましくは、記憶素子は、当該ハードディスクユニットから着脱可能である。

【0021】好ましくは、ハードディスクユニットは、機密データの入出力処理に関するデータの授受をインタフェースと記憶素子との間で仲介し、非機密データの入出力処理に関するデータの授受をインタフェースと記憶読出処理部の間で仲介する選択部をさらに備える。

【0022】好ましくは、インタフェースは、機密データを外部との間で授受する第1のインタフェースと、非機密データを外部との間で授受するための第2のインタフェースとを含み、端子は、他の装置とデータをやり取りする第1の端子と、第1の端子を第1のインタフェースに接続する第1のデータバスと、他の装置とデータをやり取りする第1の端子から独立した第2の端子と、第

2の端子を第2のインタフェースに接続する第2のデータバスを含む。

【0023】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0024】図1は、本発明によるデータ保護機能を備えたハードディスクユニットに対して、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するライセンスを記憶するための構成を示した概略図である。

【0025】コンテンツ提供装置30は、ハードディスクユニット40に記録する暗号化コンテンツデータおよびライセンスを提供する装置であり、データバスBSを介してハードディスクユニット40と接続され、データバスBSを介してデータの授受を行なえる構成となっている。

【0026】なお、以下では、デジタル通信網、たとえば、インターネットを介して映像データをダウンロードしてハードディスクユニット40に記録する配信システムを例にとって説明するが、以下の説明から明らかなように、本発明は、このような場合に限定されることなく、生データを取り込んで暗号化コンテンツデータおよびライセンスを生成し、その生成した暗号化コンテンツデータおよびライセンスをハードディスクユニット40に記憶するデータレコーダや、放送網を介して受信した暗号化コンテンツデータやライセンスをハードディスクユニット40に記憶する放送受信システム、放送網を介して暗号化コンテンツデータを取得し、デジタル通信網を介してライセンスを取得する複合配信システムなど様々な構成が考えられる。すなわち、コンテンツ提供装置30は、暗号化コンテンツデータおよびライセンスの取得経路に限定されることなく、ハードディスクユニット40との間で、データの授受を行ない、暗号化コンテンツデータとライセンスとをハードディスクユニットに送信する機能を備えている装置である。

【0027】また、映像データに限定されることなく、他の著作物としてのコンテンツデータ、たとえば、音楽データ、画像データ、朗読データ、テキストデータ、コンピュータプログラム、ゲームソフトなどを扱うことも可能なものである。

【0028】図1を参照して、データ配信システムにおいては、コンテンツ提供装置30は、ダウンロードサーバ10と端末装置20によって構成される。ハードディスクユニット40は、脱着可能なコネクタを備えた独立したユニットである。データバスBSは、端末装置20は、ハードディスクユニット40を装着する機構を介して接続可能なデータバスである。また、端末装置20は、デジタル通信網を介してコンテンツの配信を行なうダウンロードサーバ10と接続されている。

【0029】ダウンロードサーバ10は、ハードディス

クユニット40を装着した端末装置20のユーザからの配信リクエストを端末装置20から受信する。映像データを管理するダウンロードサーバ10は、配信リクエストを送信してきた端末装置20に装着されたハードディスクユニット40が正当な証明書を持つか否か、すなわち、保護機能を備えた正規の記憶装置であるか否かの認証処理を行なう。そして、ハードディスクユニット40が正規のハードディスクユニットであった場合、ダウンロードサーバ10は、ハードディスクユニット40に対して著作権を保護するために所定の暗号方式により映像データ（以下、「コンテンツデータ」とも呼ぶ。）を暗号化した暗号化コンテンツデータと、このような暗号化コンテンツデータを復号するためのコンテンツ鍵を含むライセンスとを端末装置20へ配信する。

【0030】端末装置20は、配信された暗号化コンテンツデータとライセンスを、ハードディスクユニット40に記憶するためにダウンロードサーバ10とハードディスクユニット40との仲介処理を行なう。

【0031】このとき、ライセンスの配信についてはダウンロードサーバ10とハードディスクユニット40との間にはセキュアコネクション（暗号通信路）が形成され、その中をライセンスが配信される。すなわち、ライセンスは、ハードディスクユニット40においてのみ、復号可能な暗号化が行なわれて配信され、ハードディスクユニット40において復号され、記憶される。セキュアコネクションの形成については後に詳細に説明する。このようなライセンスをハードディスクユニット40へ記憶する処理を「書込」と称することとする。

【0032】さらに、端末装置20に再生機能を備えれば、ハードディスクユニット40に記憶された暗号化コンテンツデータとそのライセンスを読み出して再生することが可能である。図2は、端末装置20が再生機能を備え、ハードディスクユニット40に記憶された暗号化コンテンツデータとそのライセンスを読み出して再生するための構成を示した概略ブロック図である。

【0033】図2を参照して、端末装置20は、端末装置内部の制御およびデータバスBSを介したハードディスクユニット40とのデータの送受信を制御するコントローラ1106と、暗号化コンテンツデータとライセンスによってコンテンツの再生を行なうデータ保護機能を備えた再生回路1550によって構成される。コンテンツの再生時においても、ハードディスクユニット40と再生回路1550との間にはセキュアコネクションが形成され、その中を再生に使用されるライセンスがハードディスクユニット40から再生回路1550に送信される。このとき、ハードディスクユニット40において再生回路1550の正当性の確認が再生回路1550の証明書の認証処理によって行なわれる。再生回路1550に対してコンテンツ鍵を送信し、暗号化コンテンツデータの再生に備える処理を「使用許諾」と称することとす

る。詳細については後述する。

【0034】さらに、ダウンロードサーバ10から受信し、ハードディスクユニット40に記憶された暗号化コンテンツデータおよびライセンスは、他のハードディスクユニットへ送信することもできる。図3は、端末装置20に備えられたデータバスBSに2台のハードディスクユニットを接続したハードディスクユニット間での暗号化コンテンツデータおよびライセンスの送信をするための構成を示した概略ブロック図である。

【0035】ハードディスクユニット40と同一の機能を備えるハードディスクユニット41が、データバスBSに接続されている。端末装置20のコントローラは、2つのハードディスクユニット40、41間のデータの送受信の制御とデータの仲介を行なう。また、ライセンスの送信に当たっては、ハードディスクユニット40とハードディスクユニット41の間にはセキュアコネクションが形成され、その中をライセンスが送信される。このとき、ハードディスクユニット40において、ハードディスクユニット41の正当性の確認がハードディスクユニット41の証明書の認証処理によって行なわれる。このような、2つのハードディスクユニット間でライセンスの送信を行なう場合に、ライセンスの送信元であるハードディスクユニット40側の処理を「複製／移動」と称することとする。また、複製／移動においては、ライセンスが複製されるか移動されるかはライセンスの内に記載される制御情報に従う。このとき、ライセンスの受信先のハードディスクユニット41側の処理は、図1におけるハードディスクユニット40の処理と同じ「書込」であり、端末装置20とハードディスクユニット40は、図1で示したコンテンツ提供装置30と見ることができる。詳細については後述する。

【0036】図3においては、1つの端末装置20に対して2つのハードディスクユニット40、41が接続されている構成のみを示したが、ハードディスクユニット41が他の端末装置に装着され、他の端末装置が端末装置20と通信ケーブルなどで接続され、端末装置間でデータ通信が可能であれば同様な処理を行なうことも可能である。

【0037】このような構成において、コンテンツデータの著作権を保護し、ユーザが自由にコンテンツデータを再生して楽しむためにシステム上必要とされるのは、第1には、コンテンツデータを暗号化する方式そのものであり、第2には、ライセンスの通信時におけるライセンスの漏洩を防ぐための方式であり、第3には、コンテンツデータの無断コピーによる利用を防止するためにコンテンツデータの利用方法や複製を制限する著作権保護機能である。

【0038】本発明の実施の形態においては、特に、配信、複製／移動および使用許諾の各処理の発生時において、これらのライセンスの出力先に対する認証およびチ

ェック機能を充実させ、非認証のハードディスクユニットおよび端末装置に対するコンテンツデータの出力を防止することによってコンテンツ鍵の流出を防ぎ、著作権の保護を強化する構成を説明する。

【0039】なお、以下の説明においては、ダウンロードサーバ10から、端末装置20に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

【0040】図4は、本発明において使用されるデータ、ライセンスの特性を説明する図である。

【0041】まず、ダウンロードサーバ10より配信されるデータについて説明する。Dcは、映像データ等のコンテンツデータである。コンテンツデータDcは、コンテンツ鍵Kcで復号可能な暗号化が施される。コンテンツ鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータE(Kc, Dc)がこの形式でダウンロードサーバ10から端末装置20のユーザに配布される。

【0042】なお、以下においては、E(X, Y)という表記は、データYを暗号鍵Xにより暗号化したことを示すものとする。

【0043】さらに、ダウンロードサーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する平文情報としての付加情報Diが配布される。なお、付加情報Diは、コンテンツデータDcを識別するためのデータID(DID)を含む。

【0044】また、ライセンスとしては、コンテンツ鍵Kc、ライセンスID(LID)、データID(DID)、および制御情報AC等が存在する。

【0045】データIDは、コンテンツデータDcを識別するためのコードであり、ライセンスIDは、ダウンロードサーバ10からのライセンスの配信を管理し、個々のライセンスを識別するためのコードである。制御情報ACは、ハードディスクユニットからのライセンスまたはコンテンツ鍵を外部に出力するに当たっての制御情報であり、再生可能回数(再生のためにライセンス鍵を出力する数)、ライセンスの移動・複製に関する制限情報などがある。

【0046】以後、ライセンスIDと、データIDと、コンテンツ鍵Kcと、制御情報ACとを併せて、ライセンスLICと総称することとする。

【0047】また、以降では、簡単化のため制御情報ACは再生回数の制限を行なう制御情報である再生回数(0:再生不可、1~254:再生可能回数、255:制限無し)と、ライセンスの移動および複製を制限する移動・複製フラグ(0:移動複製禁止、1:移動のみ可、2:移動複製可)との2項目とする。

【0048】図5は、本発明においてセキュアコネクション形成のために利用されるデータ、鍵の特性を説明するための図である。

【0049】端末装置20内の再生回路1550、およびハードディスクユニット40、41には固有の公開暗号鍵 K_{Pcxy} が設けられる。ここで、公開暗号鍵 K_{Pcxy} は、機器のクラス（種類などの一定の単位）ごとに付与され、 x は、再生回路とハードディスクユニットとを識別する識別子である。機器が再生回路等の再生装置である場合 $x=p$ であり、機器がハードディスクユニットである場合 $x=m$ とする。また、 y は、機器のクラスを識別する識別子である。公開暗号鍵 K_{Pcxy} は、秘密復号鍵 K_{cxy} によって復号可能である。これら公開暗号鍵 K_{Pcxy} および秘密復号鍵 K_{cxy} は、再生回路およびハードディスクユニットの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵が共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【0050】また、ハードディスクユニットおよび再生回路の証明書として C_{xy} が設けられる。これらの証明書は、再生回路、およびハードディスクユニットのクラスごとに異なる情報を有する。

【0051】再生回路およびハードディスクユニットの証明書 C_{xy} は、 $K_{Pcxy}/l_{cxy}/E(K_a, H(K_{Pcxy}/l_{cxy}))$ の形式で出荷時に再生回路およびハードディスクユニットに記録される。なお、 l_{cxy} は、クラスごとにまとめられた機器およびクラス公開暗号鍵 K_{Pcxy} に関する情報データである。また、 $H(X)$ は、データ列 X に対する $Hash$ 関数による演算結果である X のハッシュ値を意味し、 X/Y は X と Y との連結を意味する。 $E(K_a, H(K_{Pcxy}/l_{cxy}))$ は、 K_{Pcxy}/l_{cxy} の署名データである。

【0052】 K_{Pa} はデータ配信システム全体で共通の公開認証鍵であり、クラス公開暗号鍵 K_{Pcxy} とクラス情報 l_{cxy} とを認証局においてマスタ鍵 K_a で暗号化された署名データを復号する。マスタ鍵 K_a は、認証局において証明書内の署名データを作成するために使用される秘密暗号鍵である。

【0053】また、ハードディスクユニット40、41内のデータ処理を管理するための鍵として、ハードディスクユニット40、41ごとに設定される公開暗号鍵 K_{Pomz} と、公開暗号鍵 K_{Pomz} で暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵 K_{omz} とが存在する。これらのハードディスクユニットごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵 K_{Pomz} を個別公開暗号鍵、秘密復号鍵 K_{omz} を個別秘密復号鍵と称する。 z はハードディスクユニットを識別する個々の識別子である。

【0054】ライセンスの配信、移動、複製および使用

許諾が行なわれるごとにダウンロードサーバ10、端末装置20、およびハードディスクユニット40、41において生成される共通鍵 K_{s1w} 、 K_{s2w} が用いられる。

【0055】ここで、共通鍵 K_{s1w} 、 K_{s2w} は、ダウンロードサーバ、再生回路もしくはハードディスクユニット間の通信において、セキュアコネクションを形成する通信あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。以下においては、これらの共通鍵 K_{s1w} 、 K_{s2w} を「セッション鍵」とも呼ぶこととする。また、 w は、セッションを識別するための識別子である。

【0056】セッション鍵 K_{s1w} は、ライセンスを出力する提供元あるいは送信元において発生され、セッション鍵 K_{s2w} は、ライセンスを受取る提供先あるいは受信先において発生される。具体的には、ダウンロードサーバに代表されるライセンス提供装置では K_{s1w} が、再生回路では K_{s2w} が、そして、ハードディスクユニットでは、「書込」においては K_{s2w} 、「移動／複製」においては k_{s1w} が発生される。各処理において発生したセッション鍵を交換する。機器は、他の機器において発生したセッション鍵によるデータの復号処理を行なう機能を備える。このようにセッション鍵を用いてセキュアコネクションを構築し、ライセンスの送信をセキュアコネクションを介して行なうことによって、ライセンスに関する処理のセキュリティ強度を向上させ、通信に対する攻撃からライセンスを保護することができる。

【0057】図6は、図1に示したダウンロードサーバ10の構成を示す概略ブロック図である。

【0058】ダウンロードサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータやデータID等の配信情報を保持するための情報データベース304と、携帯電話機等の端末装置の各ユーザごとにコンテンツデータへのアクセスの開始に従った課金情報を保持するための課金データベース302と、情報データベース304に保持されたコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリアとデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0059】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315によって制

御され、配信処理時にセッション鍵 K_{s1w} を発生するためのセッション鍵発生部316と、ハードディスクユニットから送られてきた認証のための認証データ $C_{xy} = K P c_{xy} // l c_{xy} // E(K a, H(K P c_{xy} // l c_{xy}))$ を復号するための公開復号鍵である認証鍵 $K P a$ を保持する認証鍵保持部313と、ハードディスクユニットから送られてきた認証のための認証データ C_{xy} を通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの認証鍵 $K P a$ によって復号処理を行なう復号処理部312と、セッション鍵発生部316により生成されたセッション鍵 K_{s1w} を復号処理部312によって得られたクラス公開暗号鍵 $K P c_{xy}$ を用いて暗号化して、バスBS1に出力するための暗号処理部318と、セッション鍵 K_{s1w} によって暗号化された上で送信されたデータをバスBS1より受けて、セッション鍵 K_{s1w} により復号処理を行なう復号処理部320を含む。

【0060】データ処理部310は、さらに、配信制御部315から与えられるコンテンツ鍵 K_c および制御情報ACを、復号処理部320によって得られたハードディスクユニットの個別公開暗号鍵 $K P o m z$ によって暗号化するための暗号処理部326と、暗号処理部326の出力を、復号処理部320から与えられるセッション鍵 K_{s2w} によってさらに暗号化してバスBS1に出力するための暗号処理部328を含む。

【0061】ダウンロードサーバ10の配信処理における動作については、後ほどフローチャートを使用して詳細に説明する。

【0062】図7は、図1および図2に示したダウンロードサーバ10への接続機能と再生回路1550を備える端末装置20の構成を説明するための概略ブロック図である。

【0063】ダウンロードサーバ10とデジタル通信網とを介して接続し、データの送受信を行なう送受信部1104と、端末装置20の各部のデータ授受を行なうためのバスBS2と、バスBS2を介して端末装置20の動作を制御するためのコントローラ1106と、外部からの指示を端末装置20に与えるための操作パネル1108と、コントローラ1106等から出力される情報をユーザに視覚情報として与えるための表示パネル1110を含む。

【0064】端末装置20は、さらに、ダウンロードサーバ10からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なハードディスクユニット40と、ハードディスクユニット40とバスBS2との間のデータの授受を制御するためのハードディスクインタフェース1200と再生回路1550を含む。

【0065】再生回路1550は、証明書 $C p 3 = K P c p 3 Z // l c p 3 // E(K a, H(K P c p 3 //$

$/ l c p 3)$ を保持する証明書保持部1500を含む。ここで、端末装置20のクラス y は、 $y=3$ であるとする。

【0066】端末装置20は、さらに、クラス固有の復号鍵である $K c p 3$ を保持する $K c p$ 保持部1502と、バスBS2から受けたデータを復号鍵 $K c p 3$ によって復号し、ハードディスクユニット40によって発生されたセッション鍵 K_{s1w} を得る復号処理部1504を含む。

【0067】端末装置20は、さらに、ハードディスクユニット40に記憶されたコンテンツデータを復号するライセンスの使用許諾を受ける使用許諾処理においてハードディスクユニット40との間でバスBS2上においてやり取りされるデータを暗号化するためのセッション鍵 K_{s2w} を乱数等により発生するセッション鍵発生部1508と、ライセンスの使用許諾においてハードディスクユニット40からコンテンツ鍵 K_c および再生制御情報を受取る際に、セッション鍵発生部1508により発生されたセッション鍵 K_{s2w} を復号処理部1504によって得られたハードディスクユニット40で生成されたセッション鍵 K_{s1w} によって暗号化し、バスBS2に出力する暗号処理部1506を含む。

【0068】端末装置20は、さらに、バスBS2上のデータをセッション鍵 K_{s2w} によって復号して、コンテンツ鍵 K_c を出力する復号処理部1510と、バスBS2より暗号化コンテンツデータ $E(K_c, D_c)$ を受けて、復号処理部1510からのコンテンツ鍵 K_c によって暗号化コンテンツデータ $E(K_c, D_c)$ を復号してコンテンツデータ D_c をコンテンツデコーダ1518へ出力する復号処理部1516を含む。

【0069】端末装置20は、さらに、復号処理部1516からの出力を受けてコンテンツデータ D_c を再生するためのコンテンツデコーダ1518と、再生された映像信号を外部へ出力する端子1530を含む。

【0070】また、ハードディスクインタフェース1200は、ATA(AT Attachment)規格に準じたインタフェースであるとする。したがって、データバスBSは、ATAバスである。

【0071】端末装置20の各構成部分の各処理における動作については、後ほどフローチャートを使用して詳細に説明する。

【0072】図8は、図1に示すハードディスクユニット40の構成を説明するための概略ブロック図である。ハードディスクユニット40は、円盤状磁気記録媒体であるハードディスク1430、1431と、ヘッド1432～1434と、支柱1435と、アーム1435A～1435Cと、モータ1436と、サーボ制御部1437と、シーク制御部1438と、記憶読出処理部1439と、記憶素子1440と、コントローラ1441と、コマンドセクタ1442と、ATA(ATA t t

achment) インタフェース1443と、端子1444を含む。

【0073】ハードディスク1430、1431は、ダウンロードサーバ10または他のハードディスクユニットから受信した暗号化コンテンツデータを記憶するための媒体である。ヘッド1432は、アーム1435Aの先端に固定されており、ハードディスク1430の一方面にデータを記憶および／または読出を行なう。また、ヘッド1433は、アーム1435Bの先端に固定されており、ハードディスク1430の他方面とハードディスク1431の一方面とにデータを記憶および／または読出を行なう。さらに、ヘッド1434は、アーム1435Cの先端に固定されており、ハードディスク1431の他方面にデータを記憶および／または読出を行なう。アーム1435A～1435Cは、支柱1435に固定されている。

【0074】モータ1436は、所定の回転数でハードディスク1430、1431を回転する。サーボ制御部1437は、コントローラ1441からの制御により所定の回転数で回転するようにモータ1436を制御する。シーク制御部1438は、コントローラ1441からの制御によりアーム1435A～1435Cをハードディスク1430、1431の径方向にシークする。記憶読出処理部1439は、コントローラ1441からの制御により暗号化コンテンツデータをアーム1435A～1435Cに固定されたヘッド1432～1434を介してハードディスク1430、1431に記憶および／または読出を行なう。

【0075】コントローラ1441は、コマンドセクタ1442から暗号化コンテンツデータを受け、その受けた暗号化コンテンツデータをハードディスク1430、1431の所定の場所に記憶および／または読出を行なうようにサーボ制御部1437、シーク制御部1438および記憶読出処理部1439を制御する。コマンドセクタ1443は、ATAインタフェース1443から暗号化コンテンツデータおよびライセンスを受け、その受けた暗号化コンテンツデータをコントローラ1441へ出力し、ライセンスを記憶素子1440へ出力する。ATAインタフェース1443は、端子1444とコマンドセクタ1442との間でデータのやり取りを行なう。端子1444は、端末装置20のハードディスクインタフェース1200との間でデータをやり取りするための端子である。

【0076】既に説明したように、ハードディスクユニット40のクラス公開暗号鍵およびクラス秘密復号鍵として $KP_{cm}y$ および $K_{cm}y$ がそれぞれ設けられ、ハードディスクユニットのクラス証明書 $C_{my} = KP_{cm}y // l_{cm}y // E(K_a, H(KP_{cm}y // l_{cm}y))$ が設けられるが、ハードディスクユニット40においては、クラス識別子 $y = 1$ で表わされるものとす

る。また、ハードディスクユニットを識別する個別識別子 z は $z = 2$ で表されるものとする。そして、これらは、ライセンスを直接管理する記憶素子1440内で管理されている。

【0077】したがって、記憶素子1440は、認証データ $C_{m1} = KP_{cm1} // l_{cm1} // E(K_a, H(KP_{cm1} // l_{cm1}))$ を保持する証明書保持部1400と、ハードディスクユニットごとに設定される固有の復号鍵である個別秘密復号鍵 K_{om2} を保持する K_{om} 保持部1402と、クラス秘密復号鍵 K_{cm1} を保持する K_{cm} 保持部1421と、個別秘密復号鍵 K_{om2} によって復号可能な公開暗号鍵 KP_{om2} を保持する KP_{om} 保持部1416を含む。

【0078】このように、ハードディスクユニットという記憶装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をハードディスクユニット単位で実行することが可能になる。

【0079】記憶素子1440は、さらに、コマンドセクタ1442と内部バスインタフェース1424との間でデータのやり取りを行なう端子1423と、端子1423との間でデータを授受する内部バスインタフェース1424と、内部バスインタフェース1424との間で信号をやり取りするバスBS3と、バスBS3に内部バスインタフェース1424から与えられるデータを、 K_{cm} 保持部1421からのクラス秘密復号鍵 K_{cm1} により復号して、書込処理においてハードディスクユニット40の外部（ライセンスの送信元）において生成されたセッション鍵 K_{s1w} を暗号処理部1416に出力する復号処理部1422と、 KP_a 保持部1414から認証鍵 KP_a を受けて、バスBS3に与えられるデータから認証鍵 KP_a による他の機器（再生回路、または他のハードディスクユニット）の証明書の正当性を判断する認証処理を行ない、認証結果をコントローラ1420に、得られたクラス公開暗号鍵を暗号処理部1410に出力する認証処理部1408と、復号処理部1422から出力されたダウンロードサーバ10が発生したセッション鍵 K_{s1w} または復号処理部1412から出力される再生回路1550が発生したセッション鍵 K_{s2w} によって、データを暗号化してバスBS3に出力する暗号処理部1406を含む。

【0080】記憶素子1440は、さらに、書込処理においてセッション鍵 K_{s1w} を、移動／複製および使用許諾の各処理においてセッション鍵 K_{s2w} を発生するセッション鍵発生部1418と、セッション鍵発生部1418が出力したセッション鍵 K_{s1w} 、 K_{s2w} を認証処理部1408によって得られるクラス公開暗号鍵 KP_{cpz} もしくは KP_{cmz} によって暗号化してバスBS3によりセッション鍵発生部1418にて生成した K_{s1w} または K_{s2w} によって暗号化コンテンツデータ

を送出する暗号処理部1410と、バスBS3よりセッション鍵Ks2wによって暗号化されたデータを受けてセッション鍵発生部1418より得たセッション鍵Ks2wによって復号する復号処理部1412と、ライセンスの使用許諾処理においてセキュアデータ記憶領域1415から読出されたコンテンツ鍵Kcを、移動/複製処理において復号処理部1412で復号された他のハードディスクユニットの個別公開暗号鍵Kpoz(z≠2)で暗号化する暗号処理部1417を含む。

【0081】記憶素子1440は、さらに、バスBS3上のデータを個別公開暗号鍵Kpom2と対をなすハードディスクユニット40の個別秘密復号鍵Kom2によって復号するための復号処理部1404と、ライセンスを記憶するセキュアデータ記憶領域1415と、バスBS3を介して外部との間でデータ授受を行ない、バスBS3との間で制御情報ACを受けて、記憶素子1440の動作を制御するためのコントローラ1420を含む。

【0082】なお、ライセンスを記憶するセキュアデータ記憶領域1415は、ハードディスクユニット40において、ハードディスク1430、1431に障害が発生してデータの読出をできない状態になった場合であっても、ライセンスの読出を保証するために、つまり、移動/複製処理が提供できるように、ハードディスク1430、1431に対する記憶/読出とは独立してアクセス可能であり、かつ、ハードディスクユニット1430、1431より安定な記録媒体である半導体メモリによって構成される。また、記憶素子1440は、セキュリティ確保の観点から、耐タンパ構造を備えた1つの半導体素子によって構成される。

【0083】なお、記憶素子1440は、ハードディスクユニット40に着脱可能な半導体素子として構成することも可能である。

【0084】ここでは、記憶素子1440は、1つの半導体素子として構成しているが、複数の半導体素子によって構成することも可能である。このような場合に、記憶素子を構成する複数の半導体素子間の配線が観測されることでライセンスが漏洩することがないように、当該半導体素子間の配線を隠さなければならない。

【0085】このように、記憶素子1440を設けることで、ライセンスに関する機密性と安全性を確保することができる。

【0086】ハードディスクユニット40は、2枚のハードディスク1430、1431を含むが、ハードディスク1430、1431にデータを記録および/または再生するとき、ハードディスク1430にデータを記録および/または再生した後にハードディスク1431にデータを記録および/または再生するように1枚づつ、データが記録および/または再生されるのではなく、複数のヘッド1432～1434が同時に同じ位置へ移動し、その移動した位置に同時にデータを記録および/ま

たは再生する。したがって、2枚のハードディスク1430、1431の全体で1つのデータ記憶領域を構成する。

【0087】図9は、ハードディスク1430、1431の全体で構成されるデータ記憶領域の構成図を示したものである。図9を参照して、データ記憶領域2000は、ユーザ領域2100と、非ユーザ領域2200とを含む。ユーザ領域2100は、データ記憶領域2110から成る。非ユーザ領域2200は、管理データ記憶領域2210から成る。

【0088】データ領域2000は、データ領域内の記録単位ごとの記録位置を指定する実アドレス0～M+Nが設けられている。ユーザ領域には、データ領域の実アドレス0～Mによって指定されるM+1個の領域が割当てられ、管理データ領域には、データ領域の実アドレスN+1～N+Mで指定されるM個の領域が割当てられる。1つのデータ領域は512バイトのデータが記録可能である。

【0089】ユーザ領域2100には、インタフェース1443を介してデータの記憶および/または読出が直接行なえる領域であり、記録位置の指定には、LBAと呼ばれる論理アドレスが用いられる。従って、ユーザ領域には2つのアドレスが存在し、外部からはLBAによって指示し、内部では実アドレスに変換して、記憶および/または読出を行なう構成となっている。このように構成することで、指定された記録位置に不良が発生し、使用不可能となっても、その不良位置を指定していたLBAに対して、不良が発生した記録位置の割当てを破棄し、予め準備しておいた代替領域を割当てることでLBAにおける連続性を保証する。また、ユーザ領域へのインタフェース1443を介したデータの記憶および/または読出は、標準ATAコマンド(ライト/リード命令)によってLBAを指定することで実行される。

【0090】図9においては、LBAは実アドレスに一致しているが、必ずしも、一致するものではないが、必ず、1つのLBAに対して1つの実アドレスが存在する。

【0091】管理データ領域2210は、先に説明した代替のための予備の領域とハードディスクユニット40内にて独自に使用される管理データが記憶される領域である。管理データが記憶される領域には、ハードディスク1430、1431に記憶したデータ記録に関する管理データ(データ領域の代替情報、エラーログ、実アドレスとLBAマッピングテーブルなど)や、コントローラ1441のプログラムの一部などが記録されている。管理データ領域2210は、インタフェース1443を介してデータの記憶および/または読出を行なうことはできない。ただし、代替処理によってLBAが割当てられた記録位置は、ユーザ領域2100の一部として利用される。

【0092】また、記憶素子1440内のセキュアデータ記憶領域1415の記録位置の指定方法として以下においては、セキュアデータ記憶領域1415は、 n 個の記録領域に対して割当てられた記録位置を示すエントリ番号によって行なうものとする。それぞれに付与されたエントリ番号を指定することでライセンスの書込、移動／複製および使用許諾処理を行なうことが可能である。

記憶素子1440へのアクセスについては、ユーザ領域2100と異なる複数の拡張ATAコマンドを一定の順序で指示することで、通信先との間にセキュアコネクションを構築し、構築後、エントリ番号を指示することでライセンスの記憶／読出を行なうものとする。コマンドセクタ1442は、ATAコマンドを確認し、標準ATAコマンドであれば、コントローラ1441へ、拡張ATAコマンドであれば記憶素子1440の端子1423、内部バスIF1424、バスBS3を介してコントローラ1420へ伝える。

【0093】セキュアデータ記憶領域1415の記録位置の指定方法として、ユーザ領域2100の論理アドレスであるLBAとは、独立したエントリ番号を用いるとして説明したが、ハードディスクユニット40の記録領域を一元管理する意味で、セキュアデータ記憶領域1415の記録位置の指定方法をデータ領域2100に割当てられたLBAと連続するLBAを割当てて管理してもよい。この場合、たとえば、エントリ番号0～ n が論理アドレスLBAの $\max LBA + 1 \sim \max LBA + n + 1$ に割当てることができる。

【0094】ハードディスクユニット41については、その構成はハードディスクユニット同一であるため説明を省略する。また、ハードディスクユニット41のクラス識別子 y は、ハードディスクユニット40と同一の $y = 1$ とし、個別識別子 z は、 $z = 4$ ($\neq 2$) とであるとする。

【0095】データ記憶領域2110は、暗号化コンテンツデータ $E(Kc, Dc)$ 、付加情報 Di 、暗号化コンテンツデータの再生リストおよびライセンスを管理するためのライセンス管理ファイルを記憶する。管理データ記憶領域2210は、データ記憶領域2110にデータを記憶および／または読出を行なうために必要な管理情報を記憶する。

【0096】以下、図1、図2および図3におけるライセンスに関する処理について詳細に説明する。

【0097】〔配信処理〕図1に示すダウンロードサーバ10からハードディスクユニット40への暗号化コンテンツデータを復号するライセンスの配信について説明する。図10および図11は、図1に示すダウンロードサーバ10からライセンスを配信する動作を説明するための第1および第2のフローチャートである。ハードディスクユニット40は、書込処理を行なっている。

【0098】図10における処理以前に、端末装置20

のユーザは、ダウンロードサーバ10に対して電話網を介して接続し、ダウンロードを希望するコンテンツに対するデータIDを取得し、ダウンロードサーバ10に対して配信要求を行なっていること、さらに、ハードディスクユニット40のセキュアデータ記憶領域1415の記憶状況を把握して、セキュアデータ記憶領域1415の空き領域を確認して、新たにライセンスを記録するセキュアデータ記憶領域1415上の記憶位置を指定する格納先のエントリ番号を決定していることを前提としている。また、本フローチャートに従ったハードディスクユニット40へのデータの入出力および支持は、拡張ATAコマンドを用いて行なわれる。

【0099】図10を参照して、端末装置20のユーザから操作パネル1108を介してライセンスの配信処理が指示される。

【0100】ライセンスの配信処理が指示されると、コントローラ1106は、バスBS2およびハードディスクインタフェース1200を介してハードディスクユニット40へ証明書の出力要求を出力する（ステップS100）。ハードディスクユニット40のコマンドセクタ1442は、端子1444、およびATAインタフェース1443を介して証明書の出力要求を受理し、その受理した証明書の出力要求を記憶素子1440の端子1423へ出力し、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して証明書の出力要求を受理する（ステップS102）。そして、コントローラ1420は、バスBS3を介して証明書保持部1400から証明書 $Cm1$ を読出し、証明書 $Cm1$ をバスBS3、内部バスインタフェース1424および端子1423を介して出力し、コマンドセクタ1442は、証明書 $Cm1$ をATAインタフェース1443および端子1444を介してハードディスクインタフェース1200へ出力する（ステップS104）。

【0101】端末装置20のコントローラ1106は、ハードディスクユニット40からの証明書 $Cm1$ をハードディスクインタフェース1200およびバスBS2を介して受理し（ステップS106）、その受理した証明書 $Cm1$ およびライセンス購入条件のデータACをダウンロードサーバ10に対して送信し（ステップS108）、ダウンロードサーバ10は、端末装置20から認証データ $Cm1$ 、およびライセンス購入条件のデータACを受理する（ステップS110）。そして、復号処理部312は、ハードディスクユニット40から出力された証明書 $Cm1 = KPcm1 // lcm1 // E(Ka, H(KPcm1 // lcm1))$ の署名データ $E(Ka, H(KPcm1 // lcm1))$ を認証鍵保持部313からの認証鍵 KPa で復号し、その復号したデータであるハッシュ値 $H(KPcm1 // lcm1)$ を配信制御部315へ出力する。配信制御部315は、証明

書Cm1のKPcm1//lcm1に対するハッシュ値を演算し、その演算したハッシュ値が復号処理部312から受けたハッシュ値H(KPcm1//lcm1)に一致するか否かを確認する。すなわち、ダウンロードサーバ10は、復号処理部312が証明書Cm1の署名データE(Ka, H(KPcm1//lcm1))を認証鍵KPaで復号できること、および配信制御部315が送信元であるハードディスクユニット40から受信したハッシュ値と自ら演算したハッシュ値とが一致することを確認することにより証明書Cm1を検証する(ステップS112)。

【0102】配信制御部315は、復号処理部312における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した証明書を受信したか否かを判断する認証処理を行なう。正当な証明書であると判断した場合、配信制御部315は、次の処理(ステップS114)へ移行する。正当な証明書でない場合には、非承認とし、エラー通知を端末装置20へ出力し(ステップS176)、端末装置20はエラー通知を受信し(ステップS178)、書込拒否により配信動作が終了する(ステップS180)。

【0103】認証の結果、正当な証明書を持つハードディスクユニットを装着した端末装置からのアクセスであることが確認されると、ダウンロードサーバ10において、配信制御部315は、ハードディスクユニット40からのクラス公開暗号鍵KPcm1を受信し(ステップS114)、配信要求のあったライセンスを識別するためのライセンスIDを生成する(ステップS116)。

【0104】その後、配信制御部315は、端末装置20から受信したライセンスの購入条件に基づいて、制御情報ACを生成し(ステップS118)、セッション鍵発生部316は、配信のためのセッション鍵Ks1aを生成する(ステップS120)。セッション鍵Ks1aは、復号処理部312によって得られたハードディスクユニット40に対応するクラス公開暗号鍵KPcm1によって、暗号処理部318によって暗号化される(ステップS122)。

【0105】配信制御部315は、ライセンスIDおよび暗号化されたセッション鍵Ks1aを、データLID//E(KPcm1, Ks1a)として、バスBS1および通信装置350を介して端末装置20へ送信する(ステップS124)。

【0106】端末装置20がデータLID//E(KPcm1, Ks1a)を受信すると(ステップS126)、コントローラ1106は、データLID//E(KPcm1, Ks1a)をバスBS2およびハードディスクインタフェース1200を介してハードディスクユニット40へ出力し(ステップS128)、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介し

てデータLID//E(KPcm1, Ks1a)を受け、その受けたデータLID//E(KPcm1, Ks1a)を端子1423へ出力する。そうすると、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してデータLID//E(KPcm1, Ks1a)を受信する(ステップS130)。そして、コントローラ1420は、バスBS3を介して暗号化データE(KPcm1, Ks1a)を復号処理部1422へ与え、復号処理部1422は、Kcm保持部1421に保持されるハードディスクユニット40に固有なクラス秘密復号鍵Kcm1によって復号処理を行なうことにより、セッション鍵Ks1aを復号し、セッション鍵Ks1aを受信する(ステップS132)。

【0107】そうすると、ダウンロードサーバ10の配信制御部315は、セッション鍵の出力要求をバスBS1および通信装置350を介して端末装置20へ送信し、端末装置20のコントローラ1106は、セッション鍵の出力要求を受信してハードディスクインタフェース1200を介してハードディスクユニット40へ送信する(ステップS134)。ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介してセッション鍵の出力要求を受け、その受けたセッション鍵の出力要求を記憶素子1440の端子1423へ出力する。そして、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してセッション鍵の出力要求を受信し、セッション鍵を発生するようにセッション鍵発生部1418を制御する。そして、セッション鍵発生部1418は、セッション鍵Ks2aを生成する(ステップS136)。

【0108】そうすると、暗号処理部1406は、復号処理部1422より切換スイッチ1425の接点Paを介して与えられるセッション鍵Ks1aによって、セッション鍵発生部1418から切換スイッチ1426の接点Pdを介して与えられるセッション鍵Ks2a、およびKPom保持部1416から切換スイッチ1426の接点Pfを介して与えられる個別公開暗号鍵KPom2を1つのデータ列として暗号化して、暗号化データE(Ks1a, Ks2a//KPom2)をバスBS3に出力する(ステップS138)。コントローラ1420は、バスBS3に出力された暗号化データE(Ks1a, Ks2a//KPom2)にライセンスID(LID)を加えたデータLID//E(Ks1a, Ks2a//KPom2)をバスBS3、内部バスインタフェース1424および端子1423を介してコマンドセクタ1442へ出力し、コマンドセクタ1442は、データLID//E(Ks1a, Ks2a//KPom2)をATAインタフェース1443および端子1444を介して端末装置20に出力する(ステップS14

0)。

【0109】そして、端末装置20は、データLID//E(Ks1a, Ks2a//KPom2)を受信し(ステップS142)、その受信したデータLID//E(Ks1a, Ks2a//KPom2)をダウンロードサーバ10に送信する(ステップS144)。

【0110】ダウンロードサーバ10は、データLID//E(Ks1a, Ks2a//KPom2)を受信し(ステップS146)、復号処理部320は、暗号化データE(Ks1a, Ks2a//KPom2)をセッション鍵Ks1aによって復号し、ハードディスクユニット40で生成されたセッション鍵Ks2a、およびハードディスクユニット40の個別公開暗号鍵KPom2を受信する(ステップS148)。

【0111】そして、配信制御部315は、データID(DID)およびコンテンツ鍵Kcを情報データベース304から取得してライセンスLICを生成する(ステップS150)。その後、配信制御部315は、生成したライセンスLIC、すなわち、ライセンスID、データID、コンテンツ鍵Kc、および制御情報ACを暗号処理部326に与え、暗号処理部326は、復号処理部320によって得られたハードディスクユニット40の個別公開暗号鍵KPom2によってライセンスLICを暗号化して暗号化データE(KPom2, LIC)を生成する(ステップS152)。

【0112】図11を参照して、暗号処理部328は、暗号処理部326からの暗号化データE(KPom2, LIC)を、復号処理部320により復号されたセッション鍵Ks2aによってさらに暗号化して暗号化データE(Ks2a, (KPom2, LIC))を生成する(ステップS154)。そして、配信制御部315は、バスBS1および通信装置350を介して暗号化データE(Ks2a, (KPom2, LIC))を端末装置20へ出力し(ステップS156)、端末装置20は、暗号化データE(Ks2a, (KPom2, LIC))を受信する(ステップS158)。

【0113】そして、端末装置20のコントローラ1106は、暗号化データE(Ks2a, (KPom2, LIC))をバスBS2およびハードディスクインタフェース1200を介してハードディスクユニット40へ出力し(ステップS160)、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介して暗号化データE(Ks2a, (KPom2, LIC))を受け、その受けた暗号化データE(Ks2a, (KPom2, LIC))を記憶素子1440の端子1423へ出力する。記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して暗号化データE(Ks2a, (KPom2, LIC))を受信する(ステップS162)。コントロ

ーラ1420は、受理した暗号化データE(Ks2a, (KPom2, LIC))をバスBS3を介して復号処理部1412に与え、復号処理部1412は、暗号化データE(Ks2a, (KPom2, LIC))をセッション鍵発生部1418からのセッション鍵Ks2aによって復号し、暗号化データE(KPom2, LIC)を受信する(ステップS164)。

【0114】そうすると、復号処理部1404は、復号処理部1412からの暗号化データE(KPom2, LIC)をKom保持部1402からの個別秘密復号鍵Kom2によって復号し、ライセンスLICを受信する(ステップS166)。コントローラ1420がライセンスLICを受信すると、端末装置20のコントローラ1106は、ライセンスLICを格納するためのエントリをバスBS2およびハードディスクインタフェース1200を介してハードディスクユニット40へ出力し(ステップS168)、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介してエントリ番号を受け、その受けたエントリ番号を記憶素子1440の端子1423へ出力する。

【0115】そうすると、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してエントリ番号を受信する(ステップS170)。そして、コントローラ1420は、既に受理したライセンスIDと、ステップS166において受理したライセンスLICに含まれるライセンスIDとが一致するかどうかを判定し(ステップS172)、両者が不一致であるときエラー通知をバスBS3、内部バスインタフェース1424および端子1423を介してコマンドセクタ1442へ出力する。そして、コマンドセクタ1442は、エラー通知をATAインタフェース1443および端子1444を介してハードディスクインタフェース1200へ出力し(ステップS174)、端末装置20のコントローラ1106は、エラー通知をハードディスクインタフェース1200およびバスBS2を介して受理し(ステップS178)、書込拒否によって配信動作が終了する(ステップS180)。

【0116】一方、ステップS172において、2つのライセンスIDが一致すると判定されたとき、コントローラ1420は、セキュアデータ記憶領域1415のうち、ステップS170において受理したエントリ番号によって指定される領域にライセンスLICを記録し(ステップS182)、一連の動作が正常に終了する(ステップS184)。

【0117】なお、上記においては説明しなかったが、ライセンスの配信処理が終了した後、端末装置20のコントローラ1106は、暗号化コンテンツデータの配信要求をダウンロードサーバ10へ送信し、ダウンロード

サーバ10は、暗号化コンテンツデータの配信要求を受信する。そして、ダウンロードサーバ10の配信制御部315は、情報データベース304より、暗号化コンテンツデータE (Kc, Dc) および付加情報Diを取得して、これらのデータをバスBS1および通信装置350を介して端末装置20へ送信する。

【0118】端末装置20は、データE (Kc, Dc) /Diを受信して、暗号化コンテンツデータE (Kc, Dc) および付加情報Diを受信する。そうすると、コントローラ1106は、暗号化コンテンツデータE (Kc, Dc) および付加情報Diを1つのコンテンツファイルとしてバスBS2およびハードディスクインタフェース1200を介してハードディスクユニット40に入力する。また、コントローラ1106は、ハードディスクユニット40に格納されたライセンスのエントリと、平文のライセンスIDと、データIDとを含み、かつ、暗号化コンテンツデータE (Kc, Dc) と付加情報Diとに対するライセンス管理ファイルを生成し、その生成したライセンス管理ファイルをバスBS2およびハードディスクインタフェース1200を介してハードディスクユニット40に入力する。そして、ハードディスクユニット40において、コマンドセクタ1442は、受理した暗号化コンテンツデータE (Kc, Dc)、付加情報Di、およびライセンス管理ファイルをコントローラ1441へ出力する。そして、コントローラ1441は、暗号化コンテンツデータE (Kc, Dc)、付加情報Di、およびライセンス管理ファイルをヘッド1432〜1434を介してハードディスク1430、1431のデータ記憶領域2110に記録するように記憶読出処理部1439を制御し、記憶読出処理部1439は、暗号化コンテンツデータE (Kc, Dc)、付加情報Di、およびライセンス管理ファイルをハードディスク1430、1431に記録する。

【0119】さらに、端末装置20のコントローラ1106は、ハードディスクユニット40のデータ記憶領域2110に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情報Diから抽出した暗号化コンテンツデータに関する情報(曲名、アーティスト名)等を追記し、全体の処理が終了する。

【0120】このようにして、端末装置20に装着されたライセンスを記憶するハードディスクユニット40が正規の証明書を保持する機器であること、同時に、公開暗号鍵Kp cm1が有効であることを確認した上でライセンスを配信することができ、不正なハードディスクユニットへのライセンスの配信を禁止することができる。

【0121】また、ダウンロードサーバおよびハードディスクユニットでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによ

て、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0122】図12は、ハードディスクユニット40のデータ記憶領域2000およびセキュアデータ記憶領域1415を示したものである。データ記憶領域2110には、再生コンテンツリストファイル160と、コンテンツファイル1611〜161kと、ライセンス管理ファイル1621〜162kとが記憶されている。コンテンツファイル1611〜161kは、受信した暗号化コンテンツデータE (Kc, Dc) と付加情報Diとを1つのファイルとして記憶する。また、ライセンス管理ファイル1621〜162kは、それぞれ、コンテンツファイル1611〜161nに対応して記憶されており、セキュアデータ記憶領域1415に記憶したライセンスLICのエントリを格納する。

【0123】ハードディスクユニット40は、ダウンロードサーバ10から暗号化コンテンツデータおよびライセンスを受信したとき、または他のハードディスクユニットから暗号化コンテンツデータおよびライセンスを複製/移動処理によって受信したとき、暗号化コンテンツデータをハードディスク1430、1431に記憶し、ライセンスをセキュアデータ記憶領域1415に記憶する。

【0124】ハードディスクユニット40に送信された暗号化コンテンツデータのライセンスはセキュアデータ記憶領域1415のエントリによって指定された領域に記憶され、ハードディスク1430、1431のデータ記憶領域2110に記憶された再生コンテンツリストファイル160のライセンス管理ファイルを読出せば、ライセンスが格納されるセキュアデータ記憶領域1415上のエントリ番号を取得でき、その取得したエントリによって対応するライセンスをセキュアデータ記憶領域1415から読出すことができる。

【0125】また、ライセンス管理ファイル1622は、点線で示されているが、実際には記憶されていないことを示す。コンテンツファイル1612は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、端末装置20が他の端末装置から暗号化コンテンツデータだけを受信した場合や、ライセンスだけを他のハードディスクユニットに移動させた場合に相当する。

【0126】さらに、コンテンツファイル1613は、点線で示されているが、これは、たとえば、端末装置20がダウンロードサーバ10から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の端末装置へ送信した場合に相当し、ライセンスはメモリ1415に存在するが暗号化コンテンツデータが存在しないことを意味する。

【0127】[ハードディスクユニット間移動/複製処

理] 上述したように、ハードディスクユニット40のデータ記憶領域2110に記憶されている暗号化コンテンツデータは、データ記憶領域2110に記憶されたデータが標準ATAコマンドによって記憶および/または読出できることから、図3に示す構成において、ハードディスクユニット40に記憶された暗号化コンテンツデータは、ハードディスクユニット41に自由に複製することができる。しかし、暗号化コンテンツデータを他のハードディスクユニット41に複製しても、その複製したコンテンツデータを復号するためのライセンスを取得しなければ複製した暗号化コンテンツデータを再生することができない。

【0128】このように、図1に示す構成において、端末装置20にハードディスクユニット40に代えてハードディスクユニット41を装着したライセンスの配信を図10および図11のフローチャートに従って受けることも可能であるが、図3に示す構成においてハードディスクユニット40に記憶されているライセンスを、ハードディスクユニット41に移動あるいは複製することができる。上述したように、ハードディスクユニット40における処理が移動/複製処理であり、ハードディスクユニット41における処理が書込処理である。

【0129】図13および図14は、図3におけるハードディスクユニット40に記録されたライセンスをハードディスクユニット41に移動/複製するための第1および第2のフローチャートである。なお、図12における処理以前に、端末装置20、21のコントローラ1106は、ユーザがライセンスの移動/複製を行なうコンテンツの指定およびライセンスの移動/複製リクエストを行なうための入力手段(図示せず)に接続され、ユーザによってなされたライセンスの移動/複製を行なうコンテンツの指定、およびライセンスの移動/複製リクエストを受取る。そして、コントローラ1106は、送信元であるハードディスクユニット40内のコンテンツリストファイル160を参照して、移動または複製を行なうライセンスのコンテンツ管理ファイルを特定し、その特定したコンテンツ管理ファイルを参照して移動または複製するライセンスが記憶されているハードディスクユニット40のセキュアデータ記憶部1415内のエントリ番号を取得していること、および受信先のハードディスクユニット41のセキュアデータ記憶部1415内の空き領域を確認し、移動または複製されたライセンスを記憶するためのエントリ番号を決定していることを前提にしている。

【0130】図13を参照して、移動/複製リクエストがユーザから指示されると、端末装置21のコントローラ1106は、証明書の出力要求をバスBSを介してハードディスクユニット41へ送信する(ステップS200)。そして、ハードディスクユニット41のコマンドセクタ1442は、端子1444およびATAインタ

フェース1443を介して証明書の出力要求を受け、その受けた証明書の出力要求を記憶素子1440の端子1423へ出力する。

【0131】そうすると、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して証明書の出力要求を受信する(ステップS202)。そして、コントローラ1420は、証明書の出力要求を受信すると、証明書保持部1400から証明書Cm1をバスBS3を介して読出し、その読出した証明書Cm1をバスBS3、内部バスインタフェース1424および端子1423を介してコマンドセクタ1442へ出力し、コマンドセクタ1442は、証明書Cm1をATAインタフェース1443および端子1444を介して端末装置21のコントローラ1106へ出力する(ステップS204)。そして、コントローラ1106は、バスBSを介して証明書Cm1を受信し(ステップS206)、バスBSを介してハードディスクユニット40へハードディスクユニット41の証明書Cm1を送信する(ステップS208)。

【0132】そうすると、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介して証明書Cm1を受信し(ステップS210)、コマンドセクタ1442は、証明書Cm1を記憶素子1440の端子1423へ出力する。記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して証明書Cm1を受け、その受けた証明書Cm1をバスBS3を介して認証処理部1408へ与える。そして、認証処理部1408は、KPa保持部1414からの認証鍵KPaによって証明書Cm1の復号処理を実行し、その復号結果をコントローラ1420へ出力する。コントローラ1420は、証明書Cm1のデータKPCm1//lcm1に対するハッシュ値を演算し、その演算したハッシュ値が認証処理部1408から受けたハッシュ値H(KPCm1//lcm1)に一致するか否かを確認する。すなわち、ハードディスクユニット40は、認証処理部1408が証明書Cm1の暗号化データE(Ka, H(KPCm1//lcm1))を認証鍵KPaで復号できること、およびコントローラ1420が送信元であるハードディスクユニット41から受信したハッシュ値と自ら演算したハッシュ値とが一致することを確認することにより証明書Cm1を検証する(ステップS212)。

【0133】正当な証明書であると判断した場合、コントローラ1420は、次の処理(ステップS214)へ移行する。正当な証明書でない場合には、非承認とし、エラー通知を端末装置20を介して端末装置21へ出力し(ステップS282)、端末装置21はエラー通知を受信し(ステップS284)、書込拒否により移動/複

製動作が終了する(ステップS286)。

【0134】認証の結果、正当な証明書を持つハードディスクユニットを装着した端末装置からのアクセスであることが確認されると、ハードディスクユニット40において、コントローラ1420は、ハードディスクユニット41からのクラス公開暗号鍵K_{Pcm1}を受信し(ステップS214)、セッション鍵K_{s1b}を生成するようにセッション鍵発生部1418を制御し、セッション鍵発生部1418はセッション鍵K_{s1b}を生成する(ステップS216)。

【0135】その後、セッション鍵K_{s1b}は、認証処理部1408によって得られたハードディスクユニット41に対応するクラス公開暗号鍵K_{Pcm1}によって、暗号処理部1410によって暗号化される(ステップS218)。

【0136】コントローラ1420は、暗号化データE(K_{Pcm1}, K_{s1b})をバスBS3を介して暗号処理部1410から受け、その受けた暗号化データE(K_{Pcm1}, K_{s1b})をバスBS3、内部バスインタフェース1424および端子1423を介してコマンドセレクト1442へ出力し、コマンドセレクト1442は、暗号化データE(K_{Pcm1}, K_{s1b})をATAインタフェース1443および端子1444を介して端末装置20, 21へ送信する(ステップS220)。

【0137】端末装置20, 21が暗号化データE(K_{Pcm1}, K_{s1b})を受信すると(ステップS222)、コントローラ1106は、暗号化データE(K_{Pcm1}, K_{s1b})に移動/複製の対象となるライセンスを識別するライセンスIDを加えたデータLID//E(K_{Pcm1}, K_{s1b})をバスBSを介してハードディスクユニット41へ出力し(ステップS224)、ハードディスクユニット41のコマンドセレクト1442は、端子1444およびATAインタフェース1443を介してデータLID//E(K_{Pcm1}, K_{s1b})を受信する(ステップS226)。そして、コマンドセレクト1442は、データLID//E(K_{Pcm1}, K_{s1b})を記憶素子1440の端子1423へ出力し、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して、データLID//E(K_{Pcm1}, K_{s1b})を受信する。コントローラ1420は、バスBS3を介して暗号化データE(K_{Pcm1}, K_{s1b})を復号処理部1422へ与え、復号処理部1422は、K_{cm}保持部1421に保持されるハードディスクユニット41に固有なクラス秘密復号鍵K_{cm1}によって復号処理を行なうことにより、セッション鍵K_{s1b}を復号し、セッション鍵K_{s1b}を受信する(ステップS228)。

【0138】そうすると、端末装置21のコントローラ1106は、セッション鍵の出力要求をバスBSを介し

てハードディスクユニット41へ出力し(ステップS230)、ハードディスクユニット41のコマンドセレクト1442は、端子1444およびATAインタフェース1443を介してセッション鍵の出力要求を受ける。そして、コマンドセレクト1442は、セッション鍵の出力要求を記憶素子1440の端子1423へ出力し、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してセッション鍵の出力要求を受信し、セッション鍵を発生するようにセッション鍵発生部1418を制御する。

【0139】セッション鍵発生部1418は、コントローラ1420の制御に応じてセッション鍵K_{s2b}を生成し(ステップS232)、暗号処理部1406は、復号処理部1422より与えられるセッション鍵K_{s1b}によって、セッション鍵発生部1418から切換スイッチ1426の接点Pdを介して与えられるセッション鍵K_{s2b}、およびK_{Pom}保持部1416から切換スイッチ1426の接点Pfを介して与えられる個別公開暗号鍵K_{Pom4}を1つのデータ列として暗号化して、暗号化データE(K_{s1b}, K_{s2b}//K_{Pom4})をバスBS3に出力する(ステップS234)。コントローラ1420は、バスBS3に出力された暗号化データE(K_{s1b}, K_{s2b}//K_{Pom4})にライセンスID(LID)を加えたデータLID//E(K_{s1b}, K_{s2b}//K_{Pom4})をバスBS3、内部バスインタフェース1424および端子1423を介してコマンドセレクト1442へ出力する。そして、コマンドセレクト1442は、データLID//E(K_{s1b}, K_{s2b}//K_{Pom4})をATAインタフェース1443および端子1444を介して端末装置20, 21に出力し(ステップS236)、端末装置20, 21は、バスBSを介してデータLID//E(K_{s1b}, K_{s2b}//K_{Pom4})を受信し(ステップS238)、その受信したデータLID//E(K_{s1b}, K_{s2b}//K_{Pom4})をハードディスクユニット40へ出力する(ステップS240)。

【0140】ハードディスクユニット40のコマンドセレクト1442は、端子1444およびATAインタフェース1443を介してデータLID//E(K_{s1b}, K_{s2b}//K_{Pom4})を受信し(ステップS242)、その受信したデータLID//E(K_{s1b}, K_{s2b}//K_{Pom4})を記憶素子1440の端子1423へ出力する。そして、記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してデータLID//E(K_{s1b}, K_{s2b}//K_{Pom4})を受け、暗号化データE(K_{s1b}, K_{s2b}//K_{Pom4})を復号処理部1412に与える。

【0141】そうすると、復号処理部1412は、暗号

化データE (Ks1b, Ks2b/KPom4) をセッション鍵Ks1bによって復号し、ハードディスクユニット41で生成されたセッション鍵Ks2b、およびハードディスクユニット41の個別公開暗号鍵KPom4を受理する(ステップS244)。

【0142】そして、端末装置20のコントローラ1106から移動/複製の対象となるライセンスLICの記憶されているエントリ番号が出力され(ステップS246)、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介してエントリ番号を受け、その受けたエントリ番号を記憶素子1440の端子1423へ出力する。記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してライセンスLICの記憶されているエントリ番号を受理する(ステップS248)。そして、コントローラ1420は、受理したエントリ番号に基づいて、セキュアデータ記憶領域1415から移動または複製の対象となるライセンスLICを取得する(ステップS250)。コントローラ1420は、取得したライセンスLICの有効フラグが有効か否かを判定する(ステップS252)。有効フラグが有効でないと判定されたとき、上述したようにコントローラ1420はエラー通知を出力し、書込拒否により移動/複製動作が終了する(ステップS282, S284, S286)。

【0143】ステップS252において、有効フラグが有効であると判定されると、コントローラ1420は、取得したライセンスLICを暗号処理部1417に与え、暗号処理部1417は、復号処理部1412からの個別公開暗号鍵KPom4によってライセンスLICを暗号化し、暗号化データE (KPom4, LIC) を生成する(ステップS254)。

【0144】図14を参照して、コントローラ1420は、ステップS250において取得したライセンスLICに含まれる制御情報ACに基づいてライセンスをハードディスクユニット41へ複製/移動することが禁止されていないか否かを確認する(ステップS256)。そして、複製/移動が禁止されているときステップS282, S284を経て書込拒否によって移動/複製の動作が終了する(ステップS286)。ライセンスの複製が許可されているときステップS260へ移行する。一方、ライセンスの移動が許可されているときコントローラ1420は、取得した有効フラグを無効に変更する(ステップS258)。

【0145】そして、ステップS256において複製が許可されていると判定されたとき、またはステップS258の後、暗号処理部1406は、暗号処理部1417からの暗号化データE (KPom4, LIC) を、復号処理部1412により復号されたセッション鍵Ks2bによってさらに暗号化して暗号化データE (Ks2b,

(KPom4, LIC)) を生成する(ステップS260)。そして、コントローラ1420は、バスBS3、内部バスインタフェース1424および端子1423を介して暗号化データE (Ks2b, (KPom4, LIC)) をコマンドセクタ1442へ出力し、コマンドセクタ1442は、暗号化データE (Ks2b, (KPom4, LIC)) をATAインタフェース1443および端子1444を介して端末装置20, 21へ出力する(ステップS262)。

【0146】そうすると、端末装置20, 21は、暗号化データE (Ks2b, (KPom4, LIC)) を受理し(ステップS264)、端末装置21のコントローラ1106は、暗号化データE (Ks2b, (KPom4, LIC)) をバスBS3介してハードディスクユニット41へ出力する(ステップS266)。そして、ハードディスクユニット41のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介して暗号化データE (Ks2b, (KPom4, LIC)) を受け、その受けた暗号化データE (Ks2b, (KPom4, LIC)) を記憶素子1440の端子1423へ出力する。

【0147】記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して暗号化データE (Ks2b, (KPom4, LIC)) を受理する(ステップS268)。コントローラ1420は、受理した暗号化データE (Ks2b, (KPom4, LIC)) をバスBS3を介して復号処理部1412に与え、復号処理部1412は、暗号化データE (Ks2b, (KPom4, LIC)) をセッション鍵発生部1418からのセッション鍵Ks2bによって復号し、暗号化データE (KPom4, LIC) を受理する(ステップS270)。

【0148】復号処理部1404は、復号処理部1412から暗号化データE (KPom4, LIC) を受け、その受けた暗号化データE (KPom4, LIC) をKom保持部1402からの個別秘密復号鍵Kom4によって復号し、ライセンスLICを受理する(ステップS272)。

【0149】端末装置21のコントローラ1106は、ライセンスLICのエントリ番号をバスBS3を介してハードディスクユニット41へ出力し(ステップS274)、ハードディスクユニット41のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介してエントリ番号を受け、その受けたエントリ番号を記憶素子1440の端子1423へ出力する。記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介してライセンスLICの格納先であるエントリ番号を受理する(ステップS276)。

【0150】そして、コントローラ1420は、ライセ

ンスLICに含まれるライセンスIDが既に受理しているライセンスIDに一致するか否かを判定し（ステップS278）、2つのライセンスIDが不一致であるときバスBS3、内部バスインタフェース1424および端子1423を介してエラー通知をコマンドセクタ1442へ出力し、コマンドセクタ1442は、エラー通知をATAインタフェース1443および端子1444を介して端末装置20、21へ出力する（ステップS280）。そして、端末装置20のコントローラ1106は、エラー通知を受理し（ステップS284）、書込拒否によって移動/複製処理が終了する（ステップS286）。

【0151】一方、ステップS278において、2つのライセンスIDが一致すると判定されたとき、コントローラ1420は、セキュアデータ記憶領域1415のうち受理したエントリ番号によって指定された領域にライセンスLICを記録し（ステップS288）、ライセンスの移動/複製動作が正常に終了する（ステップS290）。

【0152】なお、暗号化コンテンツデータのハードディスクユニット40からハードディスクユニット41への移動/複製は、ライセンスの移動/複製が終了した後、ハードディスクユニット40のデータ記憶領域2110から暗号化コンテンツデータを読み出してハードディスクユニット41へ送信することによって行なえばよい。

【0153】また、受信側のハードディスクユニット41に対しては、移動/複製したライセンスに対するライセンス管理ファイルが既に記録されている場合には、ライセンス管理ファイルに対して格納位置などの書込みを行なうことで対象のライセンス管理ファイルを更新する。また、対象となるライセンス管理ファイルがハードディスクユニット41に記録されていない場合には、新たにライセンス管理ファイルを生成し、その生成したライセンス管理ファイルを受信側のハードディスクユニット41に記録する。

【0154】このようにして、端末装置21に装着されたハードディスクユニット41が正規の機器であること、同時に、クラス公開暗号鍵K_{PCm1}が有効であることを確認した上で、正規なハードディスクユニットへの移動要求に対してのみライセンスを移動することができ、不正なハードディスクユニットへの移動を禁止することができる。

【0155】また、ハードディスクユニットで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動/複製の動作におけるセキュリティを向上させることができる。

【0156】〔使用許諾処理〕上述したように、端末装置20に装着されたハードディスクユニット40は、ダウンロードサーバ10から、直接、暗号化コンテンツデータおよびライセンスを受信できる。ハードディスクユニット40に対して、ダウンロードサーバ10から、直接、暗号化コンテンツデータを受信し、記録する処理について説明した。また、ハードディスクユニット41に対して、ハードディスクユニット40から暗号化コンテンツデータを複製によって、ライセンスを「移動/複製」という概念によって受信し、記憶する処理について説明した。

【0157】そこで、次に、これらの各種の方法によってハードディスクユニットが受信したライセンスの使用許諾について説明する。ライセンスを保持するのは、ハードディスクユニットであり、暗号化コンテンツデータを再生するのは、端末装置20の再生回路1550である。そして、再生回路1550は、暗号化コンテンツデータを再生するとき自己が正規の機器であることをハードディスクユニット40に対して証明した後、ハードディスクユニット40からライセンスを受信する。したがって、この動作は、ハードディスクユニット40にとっては、端末装置20の再生回路1550に対してライセンスの使用を許諾することに相当する。

【0158】そこで、再生回路1550におけるライセンスを用いた暗号化コンテンツデータの再生処理を再生回路1550へのライセンスの使用許諾処理と考えることにする。

【0159】図2を参照して、コントローラ1106と再生回路1550とを内蔵した端末装置20はバスBSを介してハードディスクユニット40とデータのやり取りを行ない、再生回路1550はハードディスクユニット40からライセンスの使用許諾を受ける。したがって、ライセンスの使用許諾の説明は図2に示す概念図を用いて行なう。

【0160】図15は、ハードディスクユニット40から端末装置20の再生回路1550に対する、暗号化コンテンツデータを復号するライセンスの使用許諾処理を説明するためのフローチャートである。ハードディスクユニット41を端末装置20に装着してもライセンスの使用許諾は可能であり、この場合も図15に示すフローチャートに従ってライセンスの使用許諾が行なわれる。

【0161】なお、図15における処理以前に、端末装置20のユーザは、ハードディスクユニット40のデータ記憶領域2110に記憶されている再生リストに従って、再生するコンテンツを決定し、コンテンツファイルとライセンス管理ファイルを特定し、ライセンス管理ファイルからライセンスの格納されているエントリ番号を取得していることを前提として説明する。

【0162】図15を参照して、使用許諾動作の開始とともに、端末装置20のユーザから操作パネル1108

を介して使用許諾リクエストが端末装置20にインプットされる。そうすると、コントローラ1106は、バスBS2を介して証明書の出力要求を出力し（ステップS300）、再生回路1550は、証明書の出力要求を受理する（ステップS302）。そして、再生回路1550は、証明書Cp3をコントローラ1106へ出力し（ステップS304）、コントローラ1106は、証明書Cp3を受理し（ステップS306）、バスBSを介してハードディスクユニット40へ証明書Cp3を出力する（ステップS308）。

【0163】そうすると、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介して証明書Cp3を受け、その受けた証明書Cp3を記憶素子1440の端子1423へ出力する。記憶素子1440のコントローラ1420は、端子1423、内部バスインタフェース1424およびバスBS3を介して証明書Cp3=KPcp3//lcp3//E(Ka, H(KPcp3//lcp3))を受理し（ステップS310）、認証処理部1408は、受理した証明書Cp3のうち、署名データE(Ka, H(KPcp3//lcp3))をKPa保持部1414に保持された認証鍵KPaによって復号し、その復号したハッシュ値H(KPcp3//lcp3)をコントローラ1420へ出力する。コントローラ1420は、証明書Cp3のうちデータKPcp3//lcp3に対するハッシュ値を演算し、その演算したハッシュ値が再生回路1550において演算されたハッシュ値H(KPcp3//lcp3)に一致するか否かを確認する。そして、コントローラ1420は、再生回路1550から受理した証明書Cp3のうち、署名データE(Ka, H(KPcp3//lcp3))が認証処理部1408において復号されたこと、および2つのハッシュ値が一致することを確認することにより再生回路1550から受理した証明書Cp3を検証する（ステップS312）。証明書Cp3が非承認である場合、コントローラ1420は、バスBS3、内部バスインタフェース1424および端子1423を介してコマンドセクタ1442へエラー通知を出力し、コマンドセクタ1442は、ATAインタフェース1443および端子1444を介してエラー通知を端末装置20のコントローラ1106へ出力し（ステップS370）、コントローラ1106は、エラー通知を受理する（ステップS372）。そして、使用拒否によって一連の動作が終了する（ステップS374）。

【0164】証明書が承認された場合、コントローラ1420は、再生回路1550からのクラス公開暗号鍵KPcp3を受理し（ステップS314）、セッション鍵Ks1dを生成するようにセッション鍵発生部1418を制御し、セッション鍵発生部1418はセッション鍵Ks1dを生成する（ステップS316）。

【0165】その後、セッション鍵Ks1dは、認証処理部1408によって得られた再生回路1550に対応するクラス公開暗号鍵KPcp3によって、暗号処理部1410によって暗号化される（ステップS318）。

【0166】コントローラ1420は、暗号化データE(KPcp3, Ks1d)をバスBS3を介して暗号処理部1410から受け、その受けた暗号化データE(KPcp3, Ks1d)をバスBS3、内部バスインタフェース1424および端子1423を介してコマンドセクタ1442へ出力し、コマンドセクタ1442は、暗号化データE(KPcp3, Ks1d)をATAインタフェース1443および端子1444を介して端末装置20へ送信する（ステップS320）。

【0167】端末装置20が暗号化データE(KPcp3, Ks1d)を受信すると（ステップS322）、コントローラ1106は、暗号化データE(KPcp3, Ks1d)をバスBS2を介して再生回路1550へ出力し（ステップS324）、再生回路1550は、バスBS2を介して、暗号化データE(KPcp3, Ks1d)を受理する（ステップS326）。そして、暗号化データE(KPcp3, Ks1d)は復号処理部1504に与えられ、復号処理部1504は、暗号化データE(KPcp3, Ks1d)をKcp保持部1502からのクラス秘密復号鍵Kcp3によって復号し、ハードディスクユニット40において生成されたセッション鍵Ks1dを受理する（ステップS328）。

【0168】そうすると、セッション鍵発生部1508は、使用許諾用のセッション鍵Ks2dを生成し（ステップS330）、その生成したセッション鍵Ks2dを暗号処理部1506へ出力する。暗号処理部1506は、セッション鍵発生部1508からのセッション鍵Ks2dを復号処理部1504からのセッション鍵Ks1dによって暗号化して暗号化データE(Ks1d, Ks2d)を生成し（ステップS332）、暗号化データE(Ks1d, Ks2d)をコントローラ1106へ出力する（ステップS334）。そして、コントローラ1106は、バスBS2を介して暗号化データE(Ks1d, Ks2d)を受理し（ステップS336）、バスBSを介して暗号化データE(Ks1d, Ks2d)をハードディスクユニット40へ出力する（ステップS338）。

【0169】そうすると、ハードディスクユニット40のコマンドセクタ1442は、端子1444およびATAインタフェース1443を介して暗号化データE(Ks1d, Ks2d)を受け、その受けた暗号化データE(Ks1d, Ks2d)を記憶素子1440の端子1423へ出力する。そして、記憶素子1440の復号処理部1412は、端子1423、内部バスインタフェース1424、およびバスBS3を介して暗号化データE(Ks1d, Ks2d)を受ける（ステップS34

0)。復号処理部1412は、セッション鍵発生部1418において発生されたセッション鍵Ks1dによって暗号化データE(Ks1d, Ks2d)を復号して、再生回路1550で生成されたセッション鍵Ks2dを受理する(ステップS342)。

【0170】端末装置20のコントローラ1106は、バスBSを介してハードディスクユニット40へ、事前
に取得してあったエントリ番号を出力する(ステップS344)。

【0171】ハードディスクユニット40のコマンドセ
レクタ1442は、端子1444およびATAインタフ
ェース1443を介してエントリ番号を受け、その受け
たエントリ番号を記憶素子1440の端子1423へ出
力す記憶素子1440のコントローラ1420は、端子
1423、内部バスインタフェース1424およびバス
BS3を介してエントリ番号を受理し(ステップS34
6)、セキュアデータ記憶領域1415のうち、受理し
たエントリ番号によって指定された領域に格納され
た有効フラグに基づいてライセンスの有効性を判定
する(ステップS348)。そして、ライセンスが無効
であるとき、上述したように使用拒否によって一連
の動作が終了する(ステップS370~S374)。

【0172】一方、ステップS348において、ライ
センスが有効であると判定されたとき、コントロー
ラ1420は、エントリ番号によって指定された領域
からライセンスLICを取得し(ステップS350)、そ
の取得したライセンスLICに含まれる制御情報AC
に基づいてライセンスを端末装置20の再生回路15
50へ使用許諾することが禁止されていないか否か
を確認する(ステップS352)。そして、使用許諾が
禁止されているときステップS370、S372を経て
使用拒否によって使用許諾の動作が終了する(ス
テップS374)。ライセンスの使用許諾が無制限に
許可されているときステップS356へ移行する。一
方、ライセンスの使用許諾の回数が制限されてい
るときコントローラ1420は制御情報ACの使用許
諾の回数を変更する(ステップS354)。

【0173】ステップS352において使用許諾が無
制限に許可されているとき、またはステップS354
の後、暗号処理部1406は、コンテンツ鍵Kcを復
号処理部1412により復号されたセッション鍵Ks2
dによって暗号化し、暗号化データE(Ks2d, Kc)
を生成する(ステップS356)。そして、コントロー
ラ1420は、暗号処理部1406からの暗号化データ
E(Ks2d, Kc)をバスS3、内部バスインタフェー
ス1424および端子1423を介してコマンドセレ
クタ1442へ出力し、コマンドセレクタ1442は、
暗号化データE(Ks2d, Kc)をATAインタフェー
ス1443および端子1444を介して端末装置20の
コントローラ1106へ出力し(ステップS358)、

コントローラ1106は、暗号化データE(Ks2d,
Kc)を受理する(ステップS360)。そして、コン
トローラ1106は、暗号化データE(Ks2d, K
c)をバスBS2を介して復号処理部1510に出力し
(ステップS362)、復号処理部1510は、暗号化
データE(Ks2d, Kc)を受理する(ステップS3
64)。

【0174】そうすると、復号処理部1510は、暗
号化データE(Ks2d, Kc)をセッション鍵発生部1
508からのセッション鍵Ks2dによって復号し、コ
ンテンツ鍵Kcを受理する(ステップS366)。そし
て、使用許諾の処理が正常に終了する(ステップS3
68)。

【0175】なお、ライセンスLICの再生回路155
0への使用許諾の動作が終了した後、コントローラ
1106は、ハードディスクユニット40に対して暗号
化コンテンツデータE(Kc, Dc)を要求する。そう
すると、ハードディスクユニット40のコントローラ
1441は、データ記憶領域2110から暗号化コンテ
ンツデータE(Kc, Dc)を取得し、その取得した暗
号化コンテンツデータE(Kc, Dc)をコマンドセレ
クタ1442へ出力する。そして、コマンドセレクタ
1442は、暗号化コンテンツデータE(Kc, Dc)をATA
インタフェース1443および端子1444を介して端
末装置20へ出力する。

【0176】端末装置20のコントローラ1106は、
暗号化コンテンツデータE(Kc, Dc)を取得し、バ
スBS2を介して暗号化コンテンツデータE(Kc, D
c)を再生回路1550へ与える。

【0177】そして、再生回路1550の復号処理部
1516は、暗号化コンテンツデータE(Kc, Dc)を
復号処理部1510から出力されたコンテンツ鍵Kcに
よって復号してコンテンツデータDcを取得する。

【0178】そして、復号されたコンテンツデータD
cはコンテンツデコーダ1518へ出力され、コンテ
ンツデコーダ1518は、コンテンツデータを再生し、
DA変換器1519はデジタル信号をアナログ信号に
変換して端子1530へ出力する。そして、音楽デー
タは端子1530から外部の出力装置(たとえば、テレ
ビモニタ)へ出力される。ユーザは、出力装置を
介して再生されたコンテンツを楽しむことができる。

【0179】上記においては、暗号化コンテンツ
データを復号するためのライセンスを例にして説明
したが、本発明において対象となるものは暗号化
コンテンツデータを復号するためのライセンスに限
らず、個人情報、およびクレジットカードの情報
等の同時に2個以上存在してはいけな機密性が
要求されるデータが対象となる。このようなデー
タについても、上述した各処理を行なうこと
ができる。

【0180】この場合、機密性が要求されるデー
タをラ

イセンス内のコンテンツ鍵Kcと入れ替えることにより容易に実現できる。

【0181】この発明によるハードディスクユニットは、図16に示すハードディスクユニット40Aであってもよい。図16を参照して、ハードディスクユニット40Aは、ハードディスクユニット40のコマンドセレクタ1442を削除し、端子1445を追加したものであり、その他はハードディスクユニット40と同じである。なお、記憶素子1440は、ハードディスクユニット40Aに脱着可能な半導体素子として構成することも可能である。

【0182】ハードディスクユニット40Aにおいては、ATAインタフェース1443は、端子1444とコントローラ1441との間でデータをやり取りする。また、端子1445は、記憶素子1440の端子1423との間でデータをやり取りする。

【0183】端子1444は、暗号化コンテンツデータ等の非機密データのハードディスクユニット40Aへの入出力を行なう端子であり、端子1445は、暗号化コンテンツデータを復号するためのライセンス等の機密データをハードディスクユニット40Aへ入出力するための端子である。したがって、端末装置20のコントローラ1106は、ハードディスクインタフェース1200を介して暗号化コンテンツデータをハードディスクユニット40Aの端子1444へ入出力し、ハードディスクインタフェース1200を介してライセンスをハードディスクユニット40Aの端子1445へ入出力する。そして、ハードディスクユニット40Aにおいては、端子1444から入力された暗号化コンテンツデータは、ATAインタフェース1443を介してコントローラ1441へ入力され、コントローラ1441は、暗号化コンテンツデータをハードディスク1430、1431のデータ記憶領域2110の所定の位置に記憶するようにサーボ制御部1437、シーク制御部1438および記憶読出処理部1439を制御する。また、コントローラ1441は、ハードディスク1430、1431のデータ記憶領域2110の所定の位置から暗号化コンテンツデータを読出すようにサーボ制御部1437、シーク制御部1438および記憶読出処理部1439を制御し、記憶読出処理部1439が読出した暗号化コンテンツデータを受ける。そして、コントローラ1441は、記憶読出処理部1439から受けた暗号化コンテンツデータをATAインタフェース1443および端子1444を介して端末装置20へ出力する。

【0184】一方、記憶素子1440のコントローラ1420は、端子1445、1423、内部バスインタフェース1424およびバスBS3を介して、ライセンスの受信に関する各種の処理を行ない、受信したライセンスを最終的にセキュアデータ記憶領域1415に格納する。また、コントローラ1420は、ライセンスの使用

許諾処理においては、バスBS3、内部バスインタフェース1424および端子1423、1445を介して端末装置20とやり取りし、セキュアデータ記憶領域1415に記憶されたライセンスを読出し、その読出したライセンスをバスBS3、内部バスインタフェース1424および端子1423、1445を介して端末装置20へ出力する。

【0185】したがって、ハードディスクユニット40Aを用いることにより、上述したライセンスおよび暗号化コンテンツデータの書込処理、ライセンスおよび暗号化コンテンツデータの移動/複製処理、ライセンスおよび暗号化コンテンツデータの使用許諾処理を、ライセンスに関する処理と暗号化コンテンツデータに関する処理とを並行しながら行なうことができる。そして、各処理は、上述した図10、図11、図12、図13、図14および図15に示すフローチャートに従って行なわれる。

【0186】このように、ハードディスクユニット40Aにおいては、暗号化コンテンツデータ等の非機密データのハードディスク1430、1431への入出力と、ライセンス等の機密データのセキュアデータ記憶領域1415への入出力とは独立に行なわれるので、より高速化が可能である。

【0187】上述したように、この発明によるハードディスクユニットにおいては、暗号化コンテンツデータ等の非機密データはハードディスクに記憶され、暗号化コンテンツデータを復号するためのライセンス等の機密データは機密性を有する記憶素子に記憶されるので、ハードディスクがクラッシュ等に破壊されても暗号化コンテンツデータを復号するためのライセンスをハードディスクユニットから取出すことができる。

【0188】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 コンテンツをハードディスクユニットへ記憶するためのシステムの概略構成図である。

【図2】 ハードディスクユニットに記憶されたコンテンツの再生処理を説明するための概略ブロック構成図である。

【図3】 ハードディスクユニットに記憶されたコンテンツのハードディスクユニット間の移動/複製処理を説明するための概略構成図である。

【図4】 図1に示すシステムにおいて扱われるデータ、情報などの特性を示す図である。

【図5】 図1に示すシステムにおいてデータ保護のために用いられるデータ、鍵などの特性を示す図である。

【図6】 図1に示すダウンロードサーバの構成を示す概略ブロック図である。

【図7】 図1に示す端末装置の構成を示す概略ブロック図である。

【図8】 図1に示すハードディスクユニットの構成を示すブロック図である。

【図9】 ハードディスクユニットにおける記憶領域の構成を示す図である。

【図10】 図1に示すシステムにおけるライセンスの配信処理の動作を説明するための第1のフローチャートである。

【図11】 図1に示すシステムにおけるライセンスの配信処理の動作を説明するための第2のフローチャートである。

【図12】 ハードディスクユニットにおけるコンテンツ記憶方法を説明するための図である。

【図13】 図3に示す構成においてライセンスの移動／複製処理の動作を説明するための第1のフローチャートである。

【図14】 図3に示す構成においてライセンスの移動／複製処理の動作を説明するための第2のフローチャートである。

【図15】 図2に示す構成においてライセンスの使用許諾処理の動作を説明するためのフローチャートである。

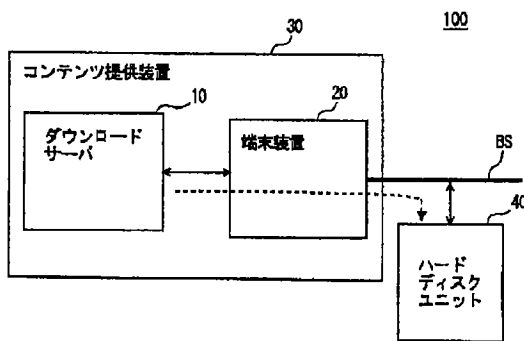
【図16】 図1に示すハードディスクユニットの他の構成を示すブロック図である。

【符号の説明】

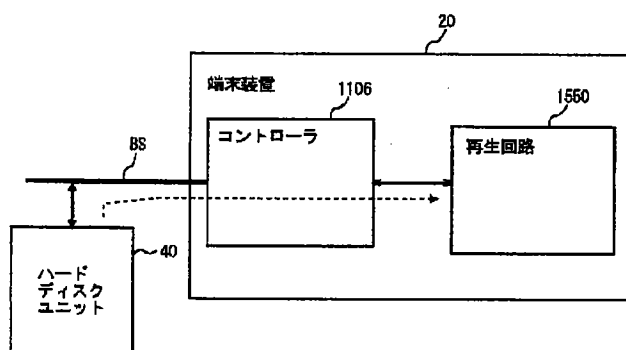
10 ダウンロードサーバ、20 端末装置、30 コンテンツ提供装置、40、41、40A ハードディスク

ユニット、100 データ配信システム、160 コンテンツリストファイル、302 課金データベース、304 情報データベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1516 復号処理部、313 認証鍵保持部、315 配信制御部、316、1418、1508 セッション鍵発生部、318、326、328、1406、1410、1417、1506 暗号処理部、350 通信装置、1106、1420、1441 コントローラ、1423、1444、1445、1530 端子、1108 操作パネル、1110 表示パネル、1200 ハードディスクインタフェース、1400、1500 証明書保持部、1402 K_{om}保持部、1414 K_{P a}保持部、1415 セキュアデータ記憶領域、1416 K_{P m c}保持部、1421 K_{c m}保持部、1430、1431 ハードディスク、1432～1434 ヘッド、1435 支柱、1435A～1435C アーム、1436 モータ、1437 サーボ制御部、1438 シーク制御部、1439 記憶読出処理部、1442 コマンドセクタ、1443 ATAインタフェース、1439 端子、1440 記憶素子、1424 内部バスインタフェース、1502 K_{c p}保持部、1518 コンテンツデコーダ、1519 DA変換器、1550 再生回路、1611～161k コンテンツファイル、1621～162k ライセンス管理ファイル、2000 データ記憶領域、2100 ユーザ領域、2110 データ記憶領域、2200 非ユーザ領域、2210 管理データ領域。

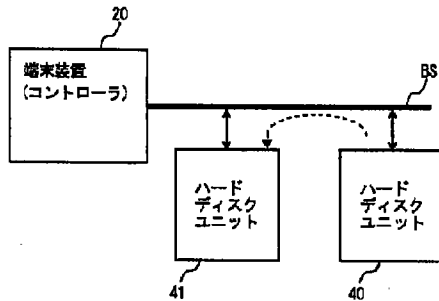
【図1】



【図2】



【図 3】



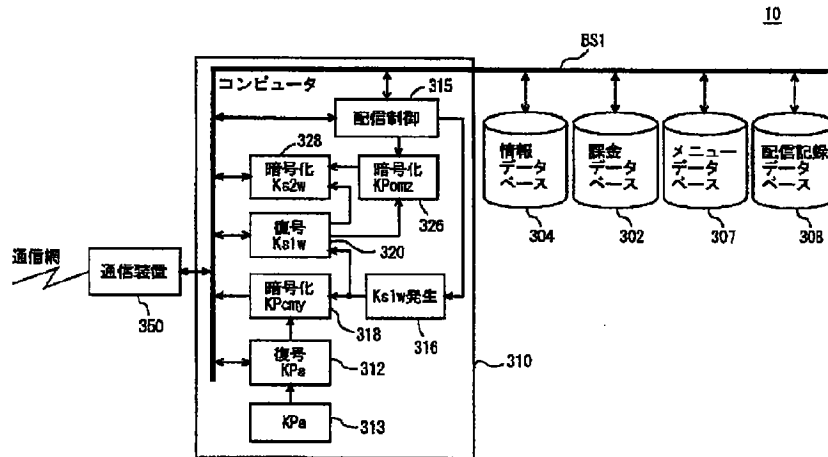
【図 4】

名称	記号	属性	特性
データ	Dc	データ固有	例：映像データ、音楽データ、図表データ、教材データ、画像データ、コンテンツ種にて暗号化した暗号化データ E(Kc, Dc) として記録管理される
データ情報	Di	データ固有	Dcに付随する平文データ。DIDを含む
データID	DID	データ固有	データおよびコンテンツ種を特定するための管理コード
コンテンツ鍵	Kc	データ固有	暗号データを暗号／復号する共通鍵
制御情報	AC	ライセンス固有	再生やライセンスの取り扱いに対する制限事項
ライセンスID	LID	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	LIC	ライセンス固有	Kc//AC//DID//LIDの総称

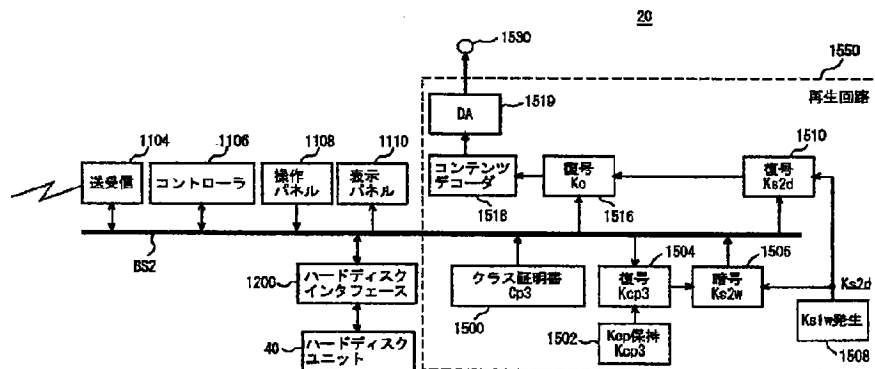
【図 5】

名称	記号	特性
マスタ鍵	Ka	クラス証明書作成のために使用する秘密暗号鍵。 認証局にて運用される
認証鍵	KPa	認証局にて証明書を検証する公開復号鍵。 ライセンス提供側にて運用される
クラス公開暗号鍵	KPox	機種のクラス（機種などの一定の単位ごと）に付与される暗号鍵。 xは機種を識別する識別子。再生装置ではp、ハードディスクユニットではmとする。 yはクラスを識別するための識別子
クラス秘密復号鍵	Koxy	クラス公開鍵KPoxにて暗号化されたデータを復号する非対称な復号鍵
クラス情報	loxy	クラスごとの機種およびクラス公開鍵に関する情報データ
クラス証明書	Oxy	$KPox // loxy // E(Ka, H(KPox // loxy))$ 認証局によってその正当性が確認できる
個別公開暗号鍵	KPmz	ハードディスクユニットごとに固有な値を持つ個別公開暗号鍵 zはハードディスクユニットを識別するための識別子
個別秘密復号鍵	Komz	個別公開鍵KPmzにて暗号化されたデータを復号する非対称な復号鍵
セッション鍵	Ks1x	ライセンスの授受ごとにライセンス提供側で生成される一時鍵 共通鍵
セッション鍵	Ks2x	ライセンスの授受ごとにライセンス受取側で生成される一時鍵 共通鍵

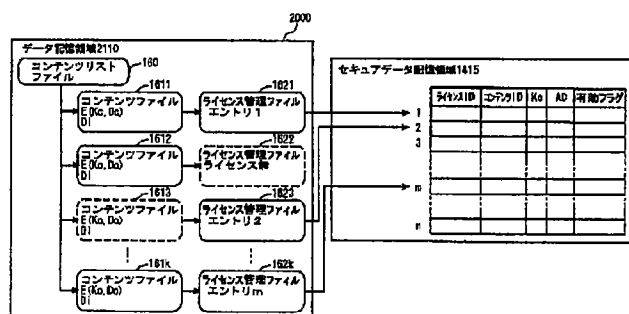
【図6】



【図7】

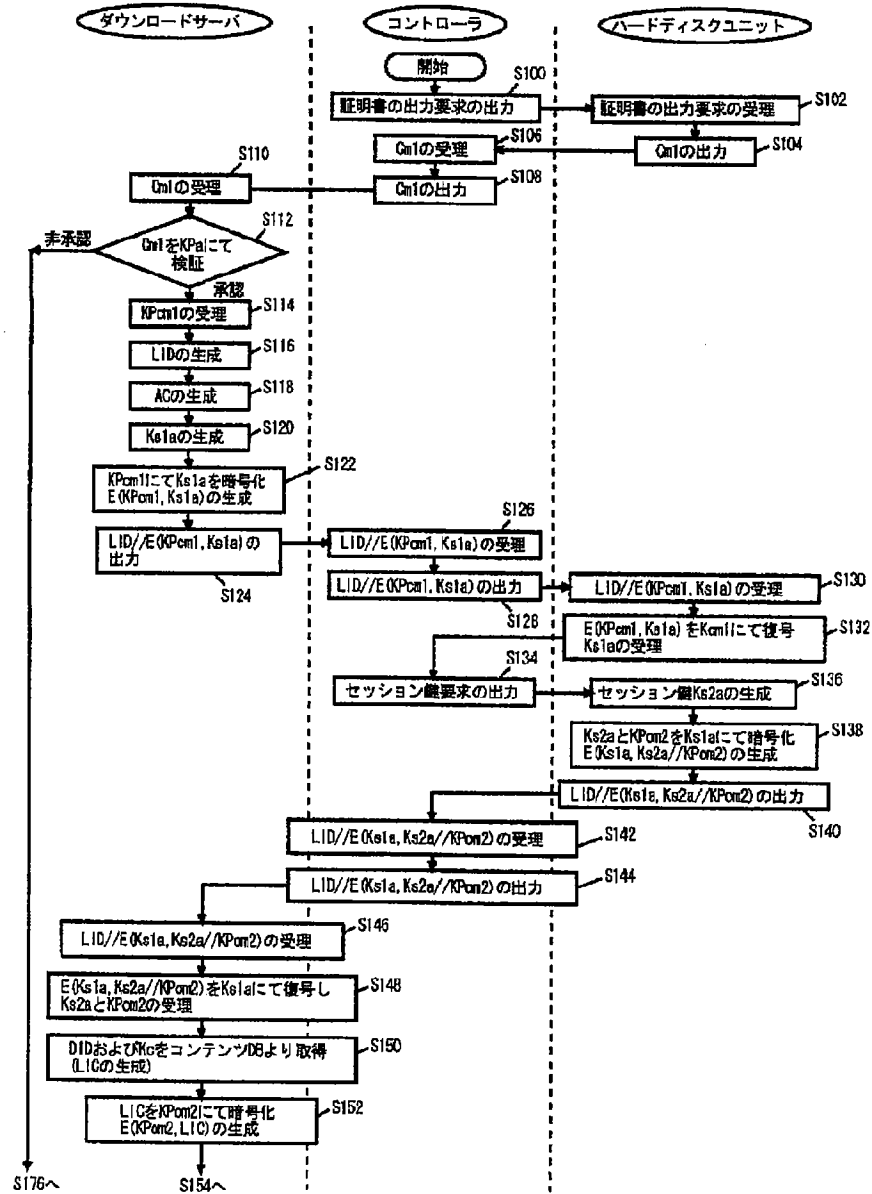


【図12】

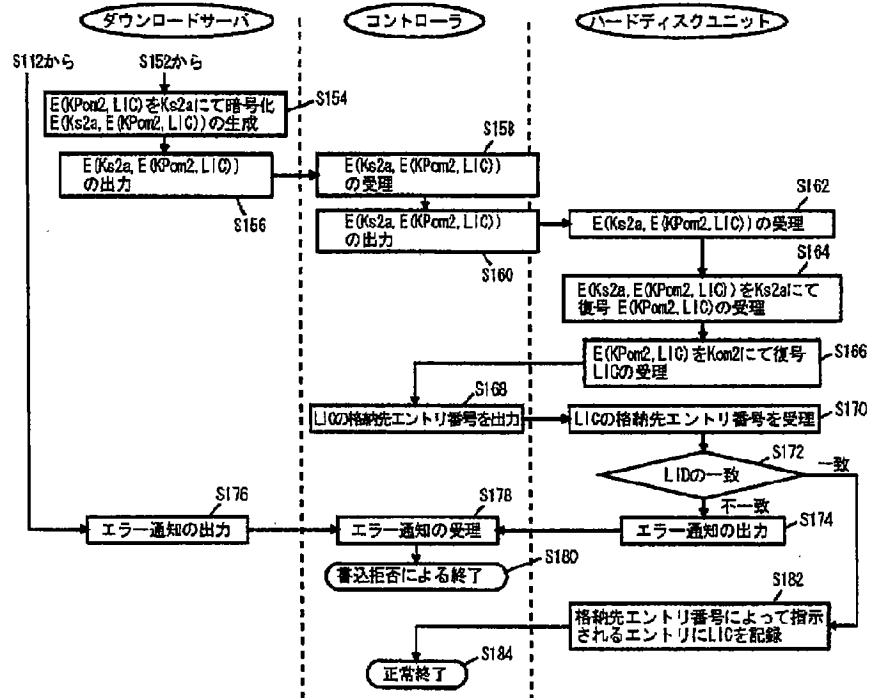


1020004

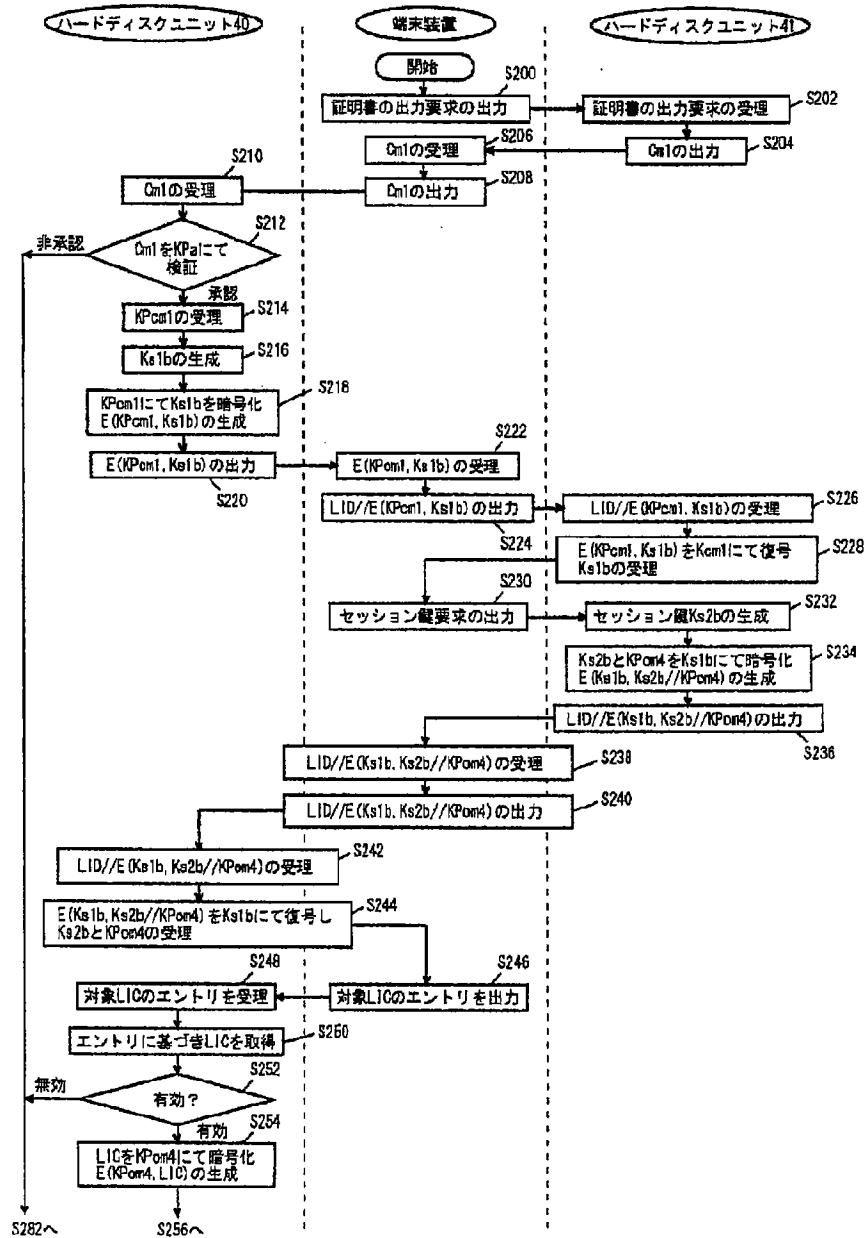
【図10】



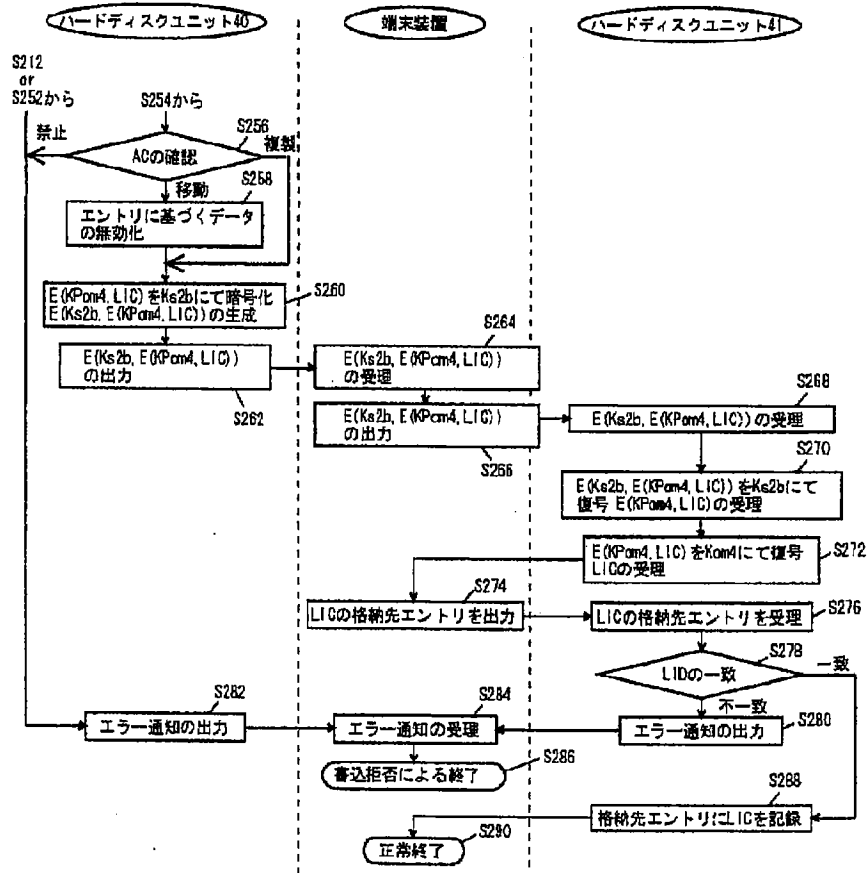
【図11】



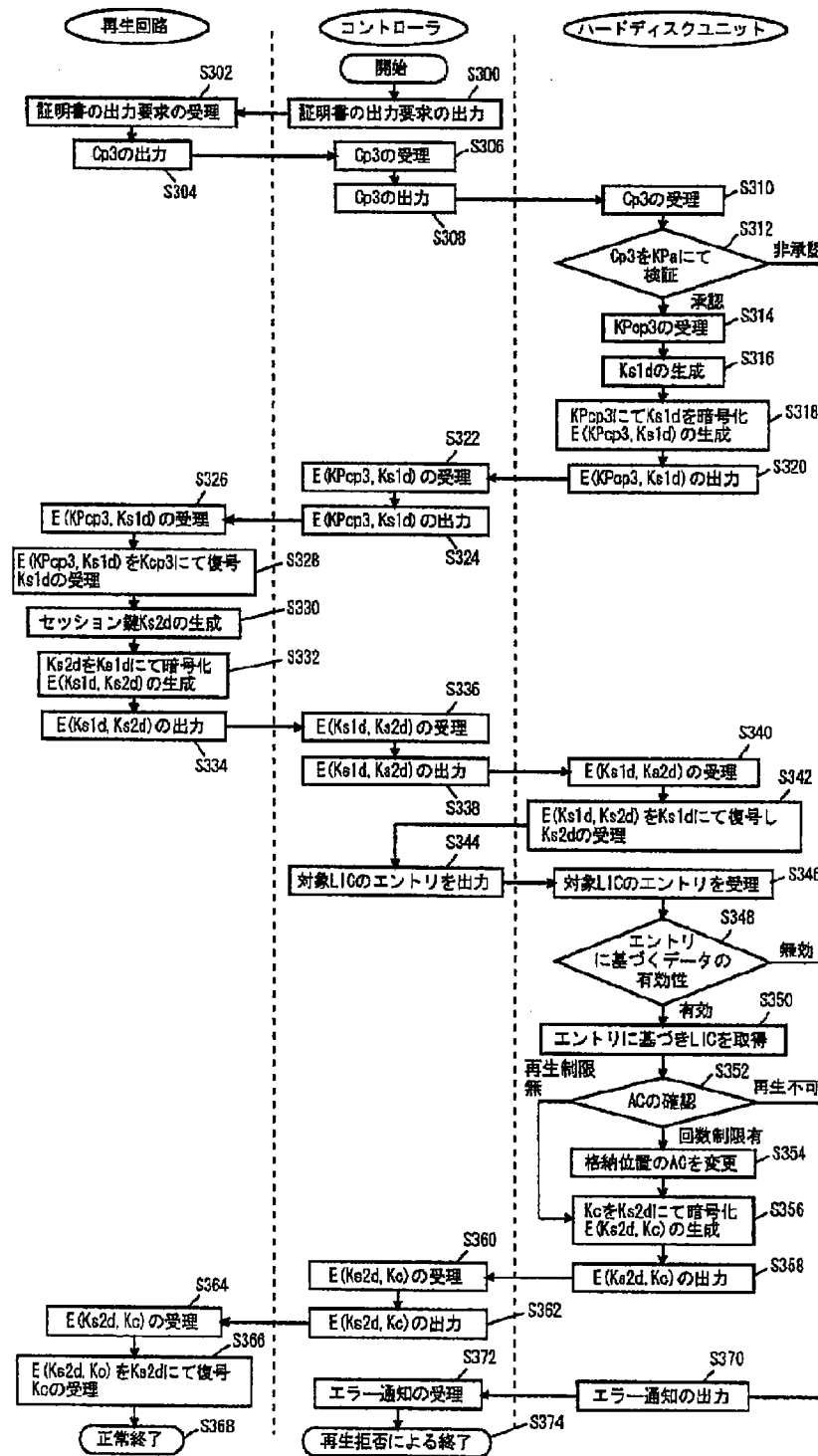
【図13】



【図 14】



【図15】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

ターム* (参考)

G 1 1 B 20/12

G 1 1 B 20/12

F ターム (参考) 5B017 AA03 BA07 CA07

5B065 BA01 BA09 PA04 PA16

5D044 BC01 BC08 CC05 CC08 DE03

DE50 EF05 FG18 GK17 HL08

HL11

5J104 AA07 AA12 EA04 KA05 NA03

NA27 NA31